VYSOKÁ ŠKOLA BÁŇSKÁ - TECHNICKÁ UNIVERZITA
OSTRAVA EKONOMICKÁ FAKULTA

Doctoral Thesis

The Security Policy Processing Method Design Based on Data life cycle.

Study Program: System Engineering and Informatics
Study branch: System Engineering and Informatics
Supervisor: Doc.Ing.Josef.Fiala.CSc

In Ostrava 2011 **Ing. Musbah Abobaker**

VYSOKÁ ŠKOLA BÁŇSKÁ
TECHNICKÁ UNIVERZITA OSTRAVA
EKONOMICKÁ FAKULTA
INSTITUT DOKTORSKCH STUDII A MBA

DECLARATION

In declare that all the work in this doctoral thesis including amendments is entirely my own unless referenced in the text as a specific source and included in the bibliography.

Date…… signature ……

Acknowledgement

I would like to thank god for his countless blessings and for giving me the opportunity to work also my family father and mother who always motivated me to do my best; wife and my children for all their love and support. I would like to thank all people helped me with this work and a special thanks to Ing. Ministr Jan, Ph.D. from TUO-EKF for being a great friend. Also a special thanks for Prof.Ing.Kaluža.Jindřich,CSc and Doc.Ing.Josef.Fiala,CSc for their support to me.

I would like to thanks my University specially my Faculty which was my home during ten years and all professors, doctors and Colleagues for all these great years together. Also i need to thanks Libya insurance company (LIC) and the top management committee for their support by giving me all the facilities to finish my work

Ing. Musbah Abobaker

Abstract

The aim of this work is to focus on Security Management from the Data Life Cycle Perspective and provide a model that can be easy understand and to implement for any organizations type.

Information life cycle management enables us to understand our data, which is an extremely valuable business asset and which must be managed properly, to ensure business success and regulatory compliance. Understanding data management means classify and determine rules, responsibility and IT requested and determine the security policy's requirement.

The work divided for two parts the theoretical part and the practical part.
The theoretical part include (the description of some theories and methods related to information security, description areas effects on information security and the description of the relation between data life cycle and the information security, and description of the model based on data life cycle and its processes)
The practical part is the implementation where the model will be in real action with one organization named Libya insurance company.

Abstrakt

Cílem disertační práce je pohled na problematiku řízení bezpečnosti pomocí Data Life Cycle. Práce zpracovává jednoduše aplikovatelný model, který lze implementovat organizacích.

Řízení životního cyklu informací nám pomáhá pochopit vlastní data, která jsou extrémně důležitá pro podnikání a musí být správně řízena, abychom zajistili podnikatelský úspěch a dodržování předpisů. Pochopení řízení dat znamená schopnost klasifikovat a nastavit pravidla, odpovědnost a IT potřeby a nastavit požadavky na bezpečnostní politiku.

Práce je členěná do dvou částí, teoretické a praktické. Teoretická část obsahuje popis některých teoretických východisek a metod vztahujících se k bezpečnosti informací. Dále popis oblastí informační bezpečnosti a popis vztahů mezi Data Life Cycle a informační bezpečností, popis modelu založeném na životním cyklu dat a jeho processech.

Praktická část je implementací, kde model bude implementován ve společnosti Libya Insurance Company.

1. Introduction

Data protection is not only the use of security equipment and software, but is more than that, the use of protective equipment needs to be used within a good knowledge of how to use and administration, the missing of the administration can guide to the risk occurrence. The security Management depends on the importance of data to the institution and the protection bases, that the last which can be summarized in technology, productivity process and the users.

The objectives of my dissertation are to design and implement the information security management method on base of data life cycle. I will start with simple definition of information security and some specific threats that identify and describe three methods of two organizations ITIL Information Technology Infrastructure Library and the FFIEC Federal Financial Institutions Examination Council. These methods look at the security from different views by the threats, business strategy and the information technology

From side of ITIL there are two perspectives, the technical and the business which means I will describe the security management from business perspective as the first method and security management from information technology perspective, and then I will go to describe the 3rd method of FFIEC the security management from risk assessment perspective. Then I finish this chapter with a definition of data life cycle.

The second is the information security implementation method sources which including comments of methods described in last part and my description side of areas of vulnerability also how I can classify and calculate the effect of damage in the end of this chapter I end up with the relation between data life cycle and security management process.

The third part is the full description of the method based on data life cycle from collecting data, creating plan to processing plan.

The forth part includes the description of the environment of implementation of my security model, which is LIC Libya Insurance Company; here will be review of company's history and description of framework and the company productivity.

Also I will go through the technology provider that there is a special situation found in Libya that there is only one provider of ITC Information Technology and Communication.

The 5th part includes the implementation of the methods to prove my methods in practice step by step describing my process and rules with documentation of each step, and result of all my work included in the Appendix at the end of this work.

2. Information Security

According to the definition of Jacques. A, Cazemier, Paul. L, Overbeek and Louk M.C. Peters in their book of data security that it is the one of the most important assets. And protection of information assets is necessary to establish and maintain trust between a company and its customers. Also timely and reliable information is necessary to process transactions and Support Company and customer. [Jacques .A, 1999]

Information security represents practice which is employed to protect information and to ensure it is available to those authorized to access it.

In general, secure systems control, through the use of specific security features, access to information that only properly authorized individuals, or processes operating on their behalf, have access to read, write, create, or delete it. Security is the mean of achieving an acceptable level of residual risks. The value of the information has to be protected. This value is determined in terms of confidentiality, integrity, and availability.

Confidentiality: protecting sensitive information from unauthorized disclosure or intelligible interception.

Integrity: safeguarding the accuracy and completeness of information and software.

Availability: ensuring that information and vital IT services are available when required. [Alison .C, 2009]

To identify the information security I found myself agrees with Albert Caballero in his Article in the handbook of computer and information security for (John. R. Vacca). That“ the Information security is a business problem in the sense that the entire organization must frame and solve security problems based on its own strategic drivers, not solely on technical controls aimed to mitigate one type of attack. The security goes beyond technical controls and encompasses people, technology, policy, and operations in a way that few other business objectives do”. [John. R.Vacca, 2009]

Exactly in the part of solving security problems based on organization’s own strategic drivers that there are no constant roles or processes, each organization has its business’s processes,

roles and acts. From that each organization has to look for the security from their view perspective.

2.1. Specific Technical Threats

This section describes specific technical threats to information security. Each of these threats functions by exploiting known vulnerabilities within computer systems. Following each of the terms presented are a description of the threat, the potential damage posed by the threat, and the countermeasures that can help to protect an organization from threat. These solutions, however, are static in nature and will remain relevant within only a limited timeframe as technical threats continually evolve. Only by realigning the focus on how businesses store sensitive data itself can government and industry effectively remove the motivation that may be shared within the hacker underground to breach systems.

2.1.1. Viruses

A virus is a computer program designed to attach itself to host files and replicate repeatedly. Viruses attach to files so that they are activated when the infected file executes (when the user opens the file). Viruses are often configured to sit in a computer's memory and infect file as the computer opens, modifies, or creates new files. [AVI, 2002]
Similar to human viruses, computer viruses usually display the following three characteristics:

- Self-replication: computer viruses are designed to continually copy themselves onto multiple host programs or files, just like a human virus travels from one person to another.
- Host program: or file just like a human virus can survive only if it infects a living person, a computer virus must inflict a host program or file.
- User activation: a computer virus will not activate and replicate until a user executes it by clicking an email attachment or visiting a malicious web page.

A. Potential damage

Viruses can harm computers by damaging programs, deleting files, or reformatting drive space. Some are not designed to do any damage at all but simply replicate themselves

and present text, video, or audio messages to the user. In addition, many viruses are poorly coded, leading to unintentional system crashes and loss.

B. Countermeasures

One of the best ways to prevent a virus infection is to restrict the opening of e-mail attachments. E-mail attachments are the number one source for virus circulation. As many viruses usurp mailing lists from infected computers to redistribute themselves, even attachments from known or trusted sources can be dangerous. Another critical protective measure is to install and use antivirus software. All organizations should consider installing antivirus software as a matter of course and require by policy that such software run automatic updates and system scans on a routing basis.[ABA, 2008],[AVI, 2002]

2.1.2. Worms

It is a computer program that self-replicates and spreads like a virus without necessarily infecting a host file. Worms consist of independent codes that exploit known system vulnerabilities without the need for a user to activate them. They self-replicate and spread without any degree of user interaction

As a result, they often are able to spread faster those viruses. For example, the structured query language (SQL).

Slammer worm Released on January 25.2003, spread globally within minutes and resulted in costs of $1 Billion. [AVI, 2002]

A. Potential Damage

A very common worm-based payload is the installation of a surreptitious “backdoor” in the infected computer, putting that computer under control of the worm author. “So big” and “my doom” are examples to threaten organizations with denial of service (DoS) attacked (attempts to make a computer resource unavailable to its intended users). In the case of the SQL slammer, the worm was able to spread so prolifically that it caused major network outages all over the world.

B. Countermeasure

Like so many other threats, worms often can be effectively prevented through the use of antivirus software. Organizations should consider installing antivirus software as a matter

of course and require by policy that such software run automatic update and system scans on a routing basis.

2.1.3. Trojan horses

The term Trojan horse is derived from homers. Seeking to gain entrance to the fortified city of troy, the Greeks built a large wooden horse near the beaches of troy and then sailed away. After Trojan soldiers brought the enormous horse into the city, Greek warriors emerged from the horse and overran troy.

As it relates to computer security, the term describes a seemingly benign program or application that contains malicious code, unbeknownst to the victim. For example, a user might download and install what appears to be a harmless freeware game, but when the program is executed, it unleashes a payload that could erase data, install a keystroke logger capable of capturing everything a user types into the keyboard, or enable a remote hacker to access the victim computer. [MS, 2009]

A. potential Damage

The potential harm from a Trojan horse is nearly limitless constrained only by the imagination of the software's authors. Once a system is infected with a Trojan horse, a malicious hacker often is able to obtain full “at the keys” access to the victim system. This ability facilitates keystroke logging, screen capturing, and any degree of data compromise resident on the victim system.

B. Countermeasure

Trojan horse programs cannot operate autonomously, as they depend on each new victim to activate them. Therefore, persons downloading or installing new software should exercise due diligence consistent with company policy, including thoroughly researching any product or application prior to installation. Because software and applications that install Trojan horses quickly earn a negative reputation on the internet, a quick internet search often can help to identify and discover these types of programs.

2.1.4. Botnets

A Botnets refers to a collection of compromised or zombie computers running malicious programs under the control infrastructure of remote commander. Commonly the perpetrator of the Botnets infrastructure has compromised a collection of remote systems busing various malware and Trojan horse tools. The presence of Botnets on the internet is steadily increasing as more and more systems fall under the control of remote hackers. Such remotely controlled computer systems are found not only in private home systems, but also in educational, corporate, government, network on an educational or corporate site where high speed connections can support a large number of other bots, completely unbeknownst to the victim organization. [AVI, 2002]

A. Potential Damage

Remote hackers can use Botnets for various malicious purposes, including DoS attacks, spam e-mail distribution, and theft of application login credentials and financial information, such as credit card and banking account information.

B. Countermeasures

Often, both kinds of software are detectable by scanning systems with updated antivirus software. All organizations; therefore, should consider installing antivirus software as a matter of course and require by policy that such software run automatic update and system scans on a routine basis.

2.1.5. Blended Threats

Blended threats are those that combine the characteristics of viruses, worms, Trojan horses, and any other malicious code designed to exploit system, vulnerabilities to initiate, transmit, and spread an attack. Due to their diverse function set, blended threats can speed rapidly and cause widespread damage to systems connected to the internet. [AVI, 2002]

A. potential damage

Because blended threats combine the use and functionality of so many other technical threats, their potential damage is enormous.

Some blended threats have combined the classical traits of a malware, which spreads rapidly without any degree of user interaction, with the traits of a Trojan horse, which grants a remote hacker full accesses to an infected system.

B. Countermeasure

The most effective protection from blended threats is a comprehensive mechanism. These mechanisms include implementing a “defense in depth” security philosophy in which an organization relies on several different protective countermeasures.

2.1.6. IP spoofing

The fundamental protocol used to send data over networks (including the internet) is internet protocol (IP). Each packet of data sent across the internet, contains the numerical source and destination IP address of that packet. By manipulating this information so that it is refer to a different or spoofed address, an attacker can falsify the original attack machine. More often than not, the system receiving the spoofed packets will send a response back to the falsified source address. [MS, 2009]

A. potential damage

IP spoofing is a common component of DoS attacks. By spoofing originating IP address, malicious hackers can effectively hide the sources(s) of such attacks. IP spoofing also is used by intruders to subvert network security layers that authenticate traffic based on IP addresses.

Across corporate networks, internal system is often configured to allow users to log in without a username or password if connecting from another system on the internal network. By spoofing a connection from a seemingly trusted machine, an attacker could potentially access the target machine without authenticating.

B. Countermeasure

Packet filtering is the most common countermeasure against IP spoofing attacks. It is recommended that a network's gateway or perimeter always perform “ingress filtering” blocking data from outside the network with a source IP address located inside the network.

Further, that same protective layer also should perform “egress is filtering” preventing data packet from leaving the network, if their IP address appears to be external to that network. Egress filtering would prevent an attacker from using internal resources to attack external machines.

2.1.7. Spam

Spam is the common term used to describe junk e-mail. The controlling the assault of non-solicited pornography and marketing act of 2003 (can-Spam act) defines Spam as “any unsolicited e-mail message the primary purpose of which is the commercial advertisement or promotion of a commercial product or service”. Spam is distributed for that Internet service.

Those who send spam use several techniques to obtain usable and legitimate e-mail addresses against which they can launch campaigns.

They often pay high dollar amounts for mailing lists with verified working and active e-mail addresses. They also use a variety of tools that scour the internet looking for e-mail addresses posted publicly on web sites and message boards. The CAN-SPAM act, designed to protect American consumers from the continued receipt of mass spam message, establishes strict guidelines that commercial e-mailers must follow to continue their practices legally. [MS, 2009], [Aycock John, 2011]

A. Potential Damage

In 2003, United States organizations incurred more that $10 billion in costs due to spam. This figure took into account lost productivity and the additional equipment, software, and related resources necessary to address the problem. Those costs are only likely to grow giving the steady, if not increased, a flow of spam since then. [AVI, 2002]

Spam also is costly in terms of its consumption of computer resources, network resources, and the time and attention is necessary to recognize and discard unwanted message. The greatest cost of spam, however, is borne by it is victims. These costs are related to the spamming itself and other crimes that usually accompany it, such as financial fraud, identity fraud, data and intellectual property theft, virus and other malware propagation, child pornography, and of course deceptive marketing .

B. Countermeasure

The most effective countermeasure to spam is being mindful of the various ways in which spammer may be attempting to obtain personal information. For example, when posting an e-mail address to a web site or message board, consider masking it .Instead of posting a full address, spell out some of the operative symbols so that address is not easily recognized as an e-mail address, such as using "your name at yahoo.com" instead of yourname@yahoo.com) any able reason, human will be able to determine your email address, but it will not be harvested by web bots.

Additionally, most e-mail programs now come equipped with an automatic spam filtering function. ISPs frequently install similar mail filters in their email transfer agents as a service to all of their customers.

Private organizations also should consider using spam filters to help protect their employees and their information technology assets.

Finally, organizations may want to consider the extent to which Individuals within the organization should respond to Opt outs in e-mails that appear suspicious. Because a recipient's request for a removal from a spammer's mailing list actually confirms that bathe e-mail address is working and functional, an Opt out request could result in additional unwanted e-mail.

While this may not be the case in many emails, organizations may want to consider providing guidance to employees on this risk and the factors they can assess to help differentiate a suspicious e-mail from other commercial email. [Aycock John, 2011]

2.1.8. Spyware

Spyware describes any computer technology that gathers and redistributes personal information about individuals or organizations without knowledge, or more important, without their consent. The most common spyware iterations install themselves on computer systems; secretly gather information to advertisers and other interested parties.

Spyware can be installed in a computer in any number of ways, whether as part of a new software application, a "drive-by" web site, or even a computer virus. [Aycock John, 2011]

A. Potential Damage

The malicious nature of spyware often can be subversive. Some will send advertisers a report on all of the web sites that a user visits, while others will send information about the user's computing or online purchasing habits.

The potential also exists for blended spyware threats to capture more important information, such as keystrokes and credit card numbers.

B. Countermeasure

The most effective countermeasure to protect against spyware is a common sense. Users always should read the end user license agreement attached to any software that they intend to install. In the end user license agreement, many programs indicate upfront that they include spyware components. Another way to protect against spyware is to run antispyware applications that can identify and remove the spyware. Most modern antivirus applications now work to detect and remove spyware.

Thus, organization should consider installing antivirus software as a matter of course and require by policy that such software run automatic updates and system scans on routing basis

2.2. The Methods of Security Management

Here in my work I will go through two philosophies of the Security Management of information Technology Infrastructure Library (ITIL) and Federal Financial Institutions Examination Council (FFIEC), describing and analyzing their methods and philosophy to determine requirements of security then I will give my opinion as a Conclusion

2.2.1. IT Infrastructure Library ” ITIL”

ITIL is a public framework that describes Best Practice in IT service management. It provides a framework for the governance of IT, the ‘service wrap’, and focuses on the continual measurement and improvement of the quality of IT service delivered, from both a business and a customer perspective. ITIL is owned by the Office of Government Commerce (OGC) and is copyright and trademark protected. The IT Service Management Forum (ITSMF) is the leading, independent, not for profit, organization that is owned and run by its worldwide members – to promote and exploit the benefits [Alison .C, 2009]

2.2.2. Security Management within ITIL

Every aspect of IT Service Management has Security Management considerations. There is a specific relationship with Availability Management - one of the prime aspects of security is Availability - and through this Business Continuity, but this should not be allowed to detract from its importance throughout the Service Management scenario. [Jacques. A, 1999]

As my understanding of the philosophy of the security management in ITIL that they look for the security management from two sides:

- Business perspective
- Information technology perspective

2.2.2.1. Information security from the business perspective

The organisation collects data in order to make products or supply a service. The data is stored, processed and made available at the moment it is needed. Those people concerned have to be able to count on its integrity. And it is equally important to ensure that only those who are authorised to do so can gain access to this information. By the time it is needed, confidentiality, integrity, and availability should no longer be open to discussion. An organisation must therefore organise the collection, storage, handling, processing and provision of data in such a way that these conditions are satisfied. [ISO/IEC17799, 2006]

Information and information processing are crucial to support business processes. Now IT not only supports the business but can even act as a promoter for generating more business (i.e. the opportunities presented by the Internet). Since all business has to deal with a lot of changes in the business and legal changes (country dependent), this could have a big impact on IT security requirements. Information security is an integral part of all business processes. With the right security, the business objectives are supported and their achievement is assured, even when internal or external negative influences occur or if the IT fails.

Maintaining information security is an iterative process. All the factors that influence its results (and therefore have to be acted upon) are seen as inputs. There are internal and external influences that have their effect on information security. The internal

influences are caused by decisions within the organisation. External influences are influences that come from the environment in which the business processes take place. This makes Security Management a challenge. [ISO/IEC17799, 2006]

Examples of changes in input which require adaptation of the process are:

- changes in tasks or the importance of tasks
- physical alterations, e.g. after moving premises
- environmental alterations
- changes in assessment of the IT used
- changes in business demands
- changes in legal demands
- changes in hardware and/or software
- changes in business demands
- changes in legal requirements
- changes in threats
- The introduction of new technology.

Model below shows the management model for information security, from a business' perspective.

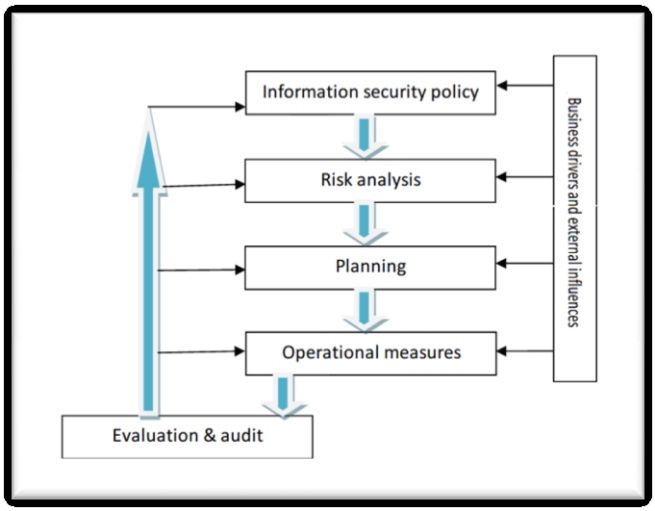

Figure 1 Security Management from Business Perspective

Top management support is a must for information security. A structured approach to information security invariably starts with the top management decision to 'do it', since it involves investments both in infrastructure and in organisation. The decision is recorded

in the information security policy, which forms the mandatory management guidelines on, among other things, the organisation, establishing the management framework, responsibilities, scope and depth. [Jacques. A, 1999]

Risk analyses may be performed to define the security needs from a business perspective as well as from a technical perspective. These analyses clarify the current status and quality of information security (the current situation) as well as the security measures that are to be implemented (the desired situation). The required situation is described in a security plan. And the method been used to analyse risk is the CCTA Risk Analysis and Management Methodology CRAM.

Planning is required to move from the current to the desired situation. After implementation, operation of the measures forms part of normal day-to-day operations. Management uses the management framework to review the effectiveness and efficiency of the implementation of the security measures. These reviews also provide the necessary feedback to either improve the implementation or improve the plan. This input is used in the periodic (yearly) security improvement plans. Of course, the results of the audits also provide input to adapt the policy, or to improve the 'tool kit' for Security Management, including, for example, the risk analysis tools.

Risk analysis helps in identifying risks and the selection of measures, it should only be applied where and when needed. Management in general is concerned about money as in cost and revenue. In information security measures, these aspects are to be treated seriously in order to avoid the image of cost-only activity. Therefore the outcome of a risk analysis should take the form of a balance, in which both risks and measures are (at least qualitatively) balanced between their 'costs' and their 'revenues'. When a risk analysis is carried out professionally, management will obtain a positive feeling about information security and is able to make decisions at the management level without the need to understand technical details. [Thomas. P, 2002], [Jacques. A, 1999]

In summary, the philosophy here is that, the information security is about assurance. A manager should feel 'in control'. Proper information security assures the continuity of the business, and the achievement of business' goals.

To secure the IT infrastructure costs money (in terms of resources, maintenance and control). Also (in terms of cost of lost production, replacement cost of stolen or damaged data/equipment, compensation payments for unachieved contractual obligations) costs money. Estimating the costs requires business knowledge in order to produce financial values. It is even more important to estimate losses because of political embarrassment, adverse publicity, and loss of customer confidence.

Effective Security Management depends on accurate risk analysis so that knowledge of the impact of risks and the costs of avoidance is understood. Without it, the tendency is either to ignore risks in the hope that they never happen, or expend disproportionate amounts of time and money on avoiding risks of minor potential impact. Risks are an inevitable feature of life, but only manageable risks should be permitted. Security management is concerned with those activities that are required to maintain the risks at manageable proportions, e.g. evaluation of effectiveness of measures, registration and trend analysis of security incidents.

2.2.2.2. Information Security from IT Management Perspective

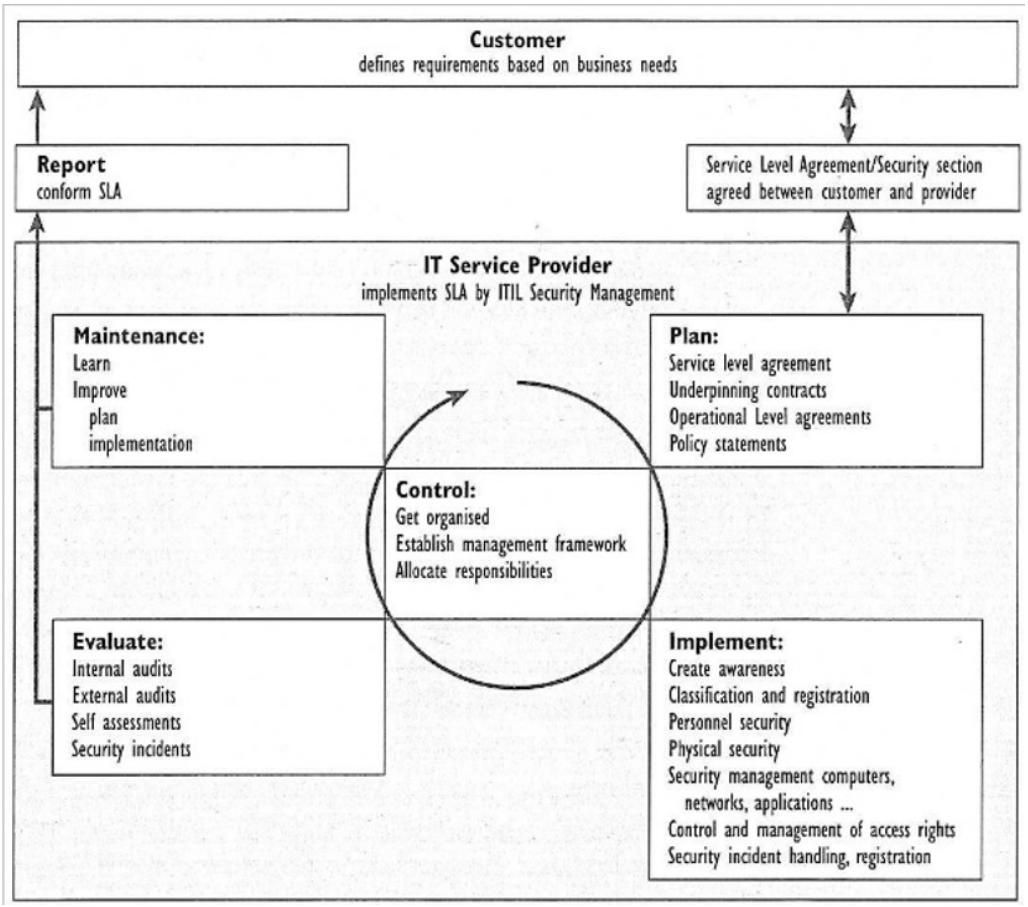

Figure 2 Information Security from it Management Perspective

For Security Management within the IT environment, the activities in the lower part of the model in Figure (1) are the most relevant (planning, operational measures, evaluation and audit), but only as far as these activities are concerned with the management of IT. The upper part and other activities (not concerning IT) addresses exactly these activities, since the authors felt it would not be right to leave these subjects out just because they do not fit neatly in the management of IT.

Figure (2) focuses on the Figure (1) activities that are relevant to the IT service provider. This figure gives an overview of the management process for the security of IT and the information in the IT environment (called the IT Security Management process). Note:

- That Figure (2) only considers the process of managing the SLA between the customer and a single service provider. Situations may arise where multiple SLA exist, sometimes with more than one service provider, and the user needs to examine to what extent this will create additional security implications and whether there is a need for inter-communication between the various service providers, possibly managed by a lead service provider or separately by the user
- That this process, like any other process, involves a closed loop.

Input for this process is the security section of the Service Level Agreement, which is the translation of the customer business needs into the specifications of the security services offered by the IT service provider. The section on security in the SLA deals with the demands for information security and the way in which these requirements are planned and implemented. The figure shows the full route from a customer requirement to the IT service provider, and back, in the form of result reports to the customer.

Note that there is no principal difference between internal and external customers or between internal and external IT service providers. An in-house IT service provider should provide just as professional a service as an outsourced IT service provider. [ISO/IEC17799, 2006]

Information security has to be controlled, planned, implemented, evaluated and maintained. Regular status reporting to the customer closes the loop. The IT Security Management process deals with information security from the perspective of IT management. Therefore, IT Security Management manages all the measures that provide the required confidence in the IT facilities.

Confidence and reliability, sufficient for the customer needs, result from the IT Security Management process. This process is further subdivided into six activities.

- **Control**

The Control activity organises and directs the IT Security Management process itself. This includes the organisation of the management framework for information security. The management framework contains the way the security plans are established, the process

through which these are implemented, the way in which the implementation is evaluated, the process through which the results of these evaluations are used for the maintenance of security plans and the implementation thereof, and, finally, the reporting structure to the customer.

The Control activity defines the (sub) processes, functions, roles, allocation of responsibilities within the sub-processes, the organisation structure between these and the reporting structure/line of command.

The Control activity is fully aligned with the control activities within the other IT management processes. The process owner for IT Security Management, called the Security Manager, is a peer to his fellow process managers. Note that, depending on the organisation, the Security Manager can be a role or a function.

- **Plan**

The Plan activity includes the way the security section of the SLA is established as well as the underpinning contracts. The generic security requirements in the SLA are refined in Operational Level Agreements (OLA). OLA is also known as 'back-to-back' agreements. They define support requirements internally (e.g., print server availability, network up-time). With respect to Security Management, these OLAs can be seen as the more detailed security plans for the organisational units of the IT service provider as well as the security handbook plans for the IT platforms.

The Plan activity may also use policy statements for the IT service provider itself (not to be confused by the policies of the customer). A policy statement could be: "every user has to be identified uniquely" or, "a basic set of security measures is offered to all customers and is always maintained".

The Plan activity within the Security Management process is aligned with the Service Level Management process in general. The Service Level Manager is leading in this effort. The Operational Level Agreements for information security (the detailed security plans) follow the normal Change Management process. The Security Manager is responsible for providing the input. But the Change Manager is responsible for the Change Management process itself. [Jacques. A, 1999]

- **Implement**

The Implement activity implements a whole range of measures as defined in the plans. In section 4 this range of activities is discussed in detail. To summarise some of the most important points:

- Maintaining awareness – Information security works because of discipline, and only when supported by clear documentation and procedures. In order to achieve effectiveness, motivation is absolutely necessary. The degree of effort required for informing and educating employees depends on the national and organisational culture. However, making security work always involves an investment.

- Security incident handling –The handling of security incidents has to be dealt with appropriately. Front doors that have been forced open cannot be left till another day. A rapid reaction is especially required when the consequences of security incidents cross organisational boundaries. Co-ordination with neighbouring organisations may be essential to locate the cause and origin of the incident.

- Security incident registration – is part of security incident control. Part of incident control knows whether similar incidents have occurred in the past and what solutions were used at the time. Security incident registration is also used to determine which part of the organisation experiences more security incidents (of a certain type) than others. This will be an indication that certain measures have to be enforced more rigorously or that different types of measures are in order. Security incident registration and handling, or, for short, security incident control, is part of the incident control process.
  Again, any changes in the infrastructure take place through the Change Management process.

- **Evaluate**

Blindly trusting security measures installed long ago will create an atmosphere of phantom security. Independent evaluation enables other parts of the organisation or third parties to have added confidence in the security measures. Evaluation results will also be used to maintain the measures taken. It might be necessary to update measures or to change measures for morel effectiveness.

Evaluation is indispensable to close the loop of the Security Management system. It concerns the status and effectiveness of measures taken; it also concerns standards and policy. Evaluating results will provide feedback on the measures in operation. It even may indicate the need for a review of the measures. When this review results in a need for change, a Request for Change (RFC) will be submitted to the Change Management process. [ISO/IEC17799, 2006], [Jacques .A, 1999]

Three types of evaluation are recognised:

- Internal audits (reviews performed by internal Electronic Data Processing (EDP) auditors)
- External audits (performed by external independent EDP auditors)
- Self assessments (performed within the line-organisation itself).

Furthermore, evaluation takes place based on the reported security incidents. These security incidents are passed to the Problem Management process for aggregation and trend analysis.

Evaluation, and in particular the information about the effectiveness of the measures provides the feedback that creates a closed-loop control system. Such a system is able to maintain and improve itself. Such a system is needed to be 'in control'.

- **Maintain**

Security measures have to be kept up to date, as the threats and the infrastructure, organisation and processes are changing constantly. Part of the maintenance effort has to be devoted to security handbooks. The books contain detailed descriptions of the measures and how to use them properly. The security handbooks have to be kept up to date, distributed and are readily available.

The maintenance of security measures is based on the results of the periodic reviews, insight into the changing risk picture, and, of course, changes in the input material (the security section in the SLA). The latter changes can also be made on the basis of new customer requirements. Another way of maintaining security measures is through the control of changes in the infrastructure as described above.

- **Report**

Reporting is an activity in itself, although it is largely dependent on the results from other actions. Reporting takes place, for example, to support the control activities or simply because this was agreed upon in the SLA (relation with the Service Level Management process).

One of the major reasons information security has been neglected for so long is the absence of historical records, i.e. historical records of the mishaps in the individual organisation.

Generally no one has any idea of what kinds of security incidents have troubled the organisation in the past. Aspects such as ignorance and the mistaken idea of not exposing the dirty linen are the most common reasons for this. There are many advantages of having a well documented security incident database. It enables a trend analysis to be made for certain types of security incidents or parts of the organisation, proves the necessity of certain measures, and provides the arguments necessary for demonstrating that specific measures are required. There is no frame of reference for management to defend the investments made in security. Risk analysis may help in some cases, but, still, investments in security can seldom be based on hard figures. And, if they can, probably something went very wrong in the past. An investment plan will most likely be based on qualitative aspects: good housekeeping, good enough to avoid public embarrassment, acceptable risk, acceptable to our customers, conform to good market principles, and conform to legal standards.

Reporting is important. Senior management of the customer has to be aware of the efficiency of the resources spent on security measures and the effectiveness of the measures. Not only the status of implementation, but also the impact of the measures has to be reported. Security incident handling can form a starting point for impact reports. [Jacques. A, 1999]

2.2.3. Federal Financial Institutions Examination Council (FFIEC) and Information Security Management

The Federal Financial Institutions Examination Council (FFIEC) was established on March 10, 1979, pursuant to title X of the Financial Institutions Regulatory and Interest Rate Control Act of 1978 (FIRA), Public Law 95-630. In 1989, title XI of the Financial Institutions Reform, Recovery and Enforcement Act of 1989 (FIRREA) established The Appraisal Subcommittee (ASC) within the Examination Council.

The Council is a formal interagency body empowered to prescribe uniform principles, standards, and report forms for the federal examination of financial institutions by the Board of Governors of the Federal Reserve System (FRB), the Federal Deposit Insurance Corporation (FDIC), the National Credit Union Administration (NCUA), the Office of the Comptroller of the Currency (OCC), and the Office of Thrift Supervision (OTS) and to make recommendations to promote uniformity in the supervision of financial institutions. The Council was given additional statutory responsibilities by section 340 of the Housing and Community Development Act of 1980 to facilitate public access to data that depository institutions must disclose under the Home Mortgage Disclosure Act of 1975 (HMDA) and the aggregation of annual HMDA data, by census tract, for each metropolitan statistical area (MSA).

The Council has established, in accordance with the requirement of the statute, an advisory State Liaison Committee composed of five representatives of state supervisory agencies. [FFIEC, 2006]

2.2.3.1. Information security from Risk Assessment perspective

Here the security process is the method an organization uses to implement and achieve its security objectives. The process is designed to identify measure, manage, and control the risks to system and data availability, integrity, and confidentiality, and to ensure accountability for system actions. The process includes five areas that serve as the framework

- **Information Security Risk**

Assessment—a process to identify and assess threats, vulnerabilities, attacks, probabilities of occurrence, and outcomes. Where must maintain an ongoing information security risk assessment program that effectively:

- Gathers data regarding the information and technology assets of the organization, threats to those assets, vulnerabilities, existing security controls and processes, and the current security standards and requirements.
- Analyzes the probability and impact associated with the known threats and vulnerabilities to their assets.
- Prioritizes the risks present due to threats and vulnerabilities to determine the appropriate level of training, controls, and assurance necessary for effective mitigation.

- **Information Security Strategy**

A plan is to mitigate risk, which integrates technology, policies, procedures, and training. The plan should be reviewed and approved by the board of directors. In other ways you should develop a strategy that defines control Objectives and establishes an implementation plan. The security strategy should include:

- Appropriate consideration of prevention, detection, and response mechanisms.
- Implementation of the least permissions and least privileges concepts.
- Layered controls that establish multiple control points between threats and organization assets.
- Policies that guide officers and employees in implementing the security program.

- **Security Controls Implementation**

The acquisition and operation of technology, the specific assignment of duties and responsibilities to managers and staff, the deployment of risk-appropriate controls, and the assurance that management and staff understand their responsibilities and have the knowledge, skills, and motivation necessary to fulfill their duties. Should have an effective process to administer access rights [FFIEC,2006]

The process should include:

- Assigning users and devices only the access required to perform their required functions.
- Updating access rights based on personnel or system changes.
- Reviewing periodically users' access rights at an appropriate frequency based on the risk to the application or system.
- Designing appropriate acceptable-use policies and require users to agree to them in writing.

- **Security Monitoring**

The use of various methodologies to gain assurance that risks are appropriately assessed and mitigated, these methodologies should verify that significant controls are effective and performing as intended. Should use effective authentication methods appropriate to the level of risk [FFIEC, 2006]

Steps include:

- Selecting authentication mechanisms based on the risk associated with the particular application or services.
- Considering whether multi-factor authentication is appropriate for each application.
- Taking into account that multifactor authentication is increasingly necessary for many forms of electronic banking and electronic payment activities.
- Encrypting the transmission and storage of authenticators (e.g., passwords, personal identification numbers (PINs), digital certificates, and biometric templates).

- **Security Process Monitoring and Updating**

The process of continuously gathering and analyzing information regarding new threats and vulnerabilities, actual attacks on the institution or others combined with the effectiveness of the existing security controls. This information is used to update the risk assessment, strategy, and controls. Monitoring and updating makes the process continuous instead of a one-time event. They should secure access to their computer networks through multiple layers of access controls to protect against unauthorized access. [FFIEC, 2006]:

- Institutions should Group network servers, applications, data, and users into security domains (e.g., entrusted external networks, external service providers, or various internal user systems).
- Establish appropriate access requirements within and between each security domain.
- Implement appropriate technological controls to meet those access requirements consistently.
- Monitor cross-domain access for security policy violations and anomalous activity.

2.3. Data Life Cycle.

As we know the information can be found in varied forms

- Printed or written on paper
- Stored electronically
- Transformed by post or electronically
- Result of conversation
- Known as skill of staff

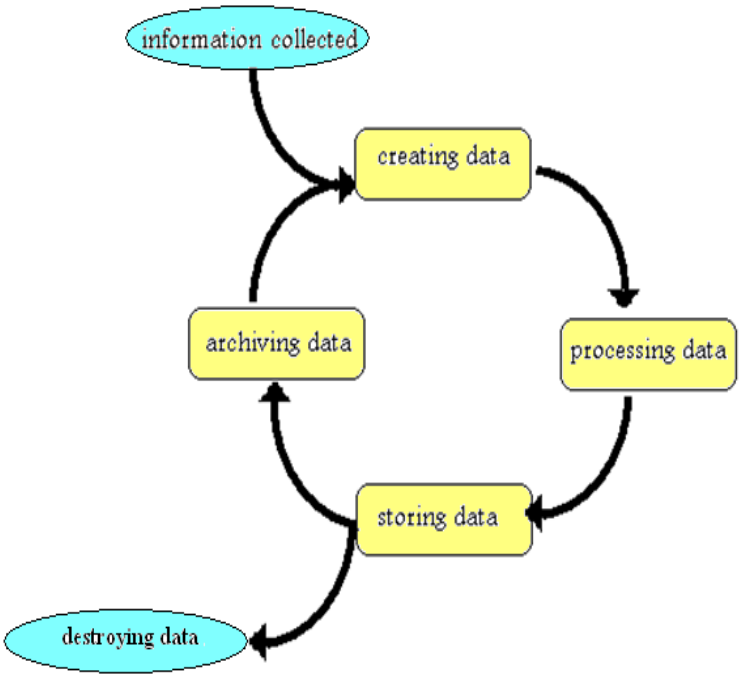

Figure 3 Information life Cycle Management

2.3.1. Creating data

Each organization has based their baseness on information as for example Libya insurance company is based on the social information collected from resources as acts, magazines and newspaper or from government organizations, society and competitors etc. This information has to be protected to keep organization in the advanced level.

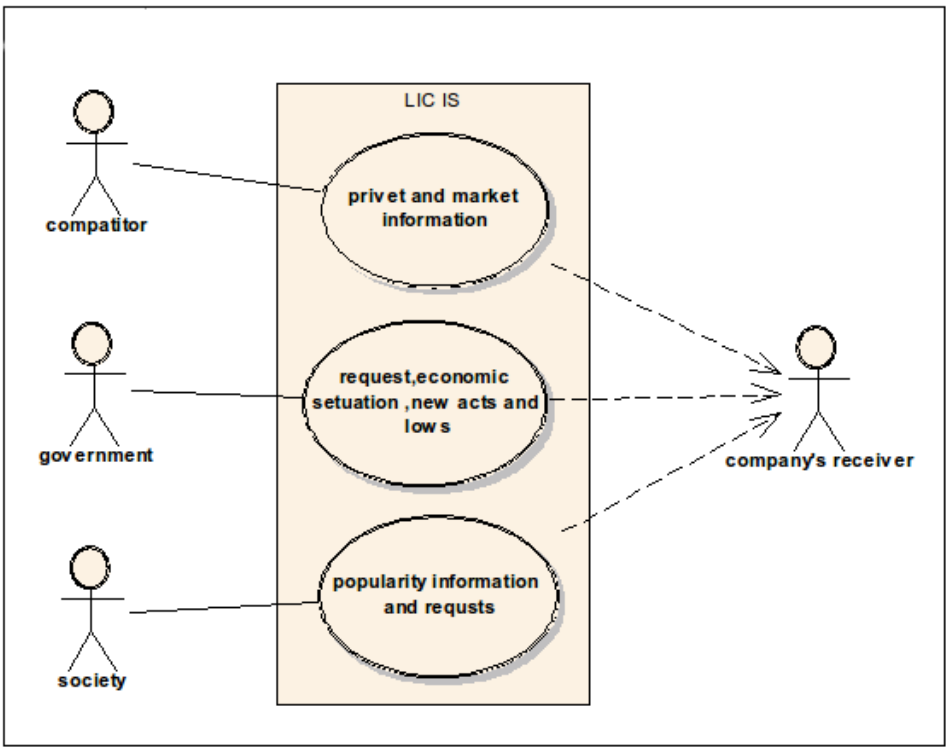

Figure 4 Relation between Data Resource and Organization

Data collected is the expensive part in business, but it has no value if doesn't transformed to the real profit. And to do that, you need to create your own data index from collected data which will give you the profit and to surpass you from other competitor.

2.3.2. Processing information

To determine the products, we have to identify the organization, in law and economics views. As an example we have the LIC with the insurance business. And Insurance business is a form of risk management primarily used to hedge against the risk of a contingent loss. Insurance is defined as the equitable transfer of the risk of a potential loss, from one entity to another, in exchange for a premium and duty of care.

Insurance in economics side is the company that sells the insurance. Insurance rate is a factor used to determine the amount, called the premium, to be charged for a certain amount of insurance coverage. And the following table shows the use case of data collected in organization.

Table 1 Summary of Data Process in Organization

Actor	Data requirement	Use case
Government	• request from government's ,industries and organizations • Information of expected future of economy • The change in acts and lows	***Data government process :*** • Studying the orders • Finding possibility • Offering the order • Informing data base • Noting economic change and analyze the risk • Participation in acts or lows magazine • Studding the changes effects
Competitors	• Prices of actions • New entry competitor • Economic life of competitors	***)ata competitor process :*** • Study a market price • Study possibility of competitor • Informing management community
Society	• Orders • Society information	***Data society process :*** • Study order • Finding possibility • Offering the order • Finding contact of people out the system • Inform data base

2.3.3. Storage or deleted information

From last table two times mentioned data base, but also there are other data have to be stored in use and other have to be archived as reports or validation data in time.
Following table describes a kind of data storage from each resource

Table 2 Data Storage from each Resource

Resources	Data storage
Government	Support data
Government	Customers data
Competitors	Competitors data
Society	Customers data

2.3.4. Archive information.

A lot of data after being used loses its value "no profit from" in that time, but may be it could help as a history for training or could be used again in future, these kind of data are stored in an archive .

2.4. Summary

Respecting their philosophy of the security management perspectives, as I Nominate and endorse with the first release of ITIL because cooperate both business and IT perspectives. But if we look at the security through the question for who's the security made? Or from other side what is the security target or goal?

Yes you will say to secure organizations resources which means, data not Technology or humans. Yes technology and human are users and tools to achieve the security and organization production; also it can be the approach to risk.

From that side I targeted in my work the data directly to achieve the real security management as we will see in the next chapter of my way with the security management from Data Life Cycle perspective.

3. Information Security Implementation Method ISIM Sources

3.1. Abstraction

As you see in the previous chapter I describe some theories which are related to my work. Here I will describe my notes and comment of each of them as a starting point to me describing the areas of security and go on to describe the relation between the data cycle and the areas of information security and how the data life cycle can be a guider of security the model came out from the combination.

3.1.1. The Philosophy From Business Perspective

"Information security is an integral part of all business processes. With the right security, the business objectives are supported and their achievement is assured, even when internal or external negative influences occur or if the IT fails". [ISO/IEC17799, 2006]

Here is described the information security as a support point of the business and not as a part of the business and from their model in figure 1 it starts with the security policy and says that it should be established depending on two things - the top management decision and the business strategy. Ok, I agree with it, but there are many things that will be missing in the policy as the processor's knowledge, skills and behavior also there are the external threats and the determination of technical requirements. In the second point there is the risk analyzes.

"These analyses clarify the current status and quality of information security (the current situation) as well as the security measures that are to be implemented". [Jacques. A, 1999]

In that point if the policy had been written without determination of threats points that will find risk point, I think it will be better to analyze the existing situation to determine the requirement and the points of risk within the system whole the system to start establishing the policy after that.

Planning point came in the model like a maintaining point as I note in the following sentences:

"Planning is required to move from the current to the desired situation. After implementation, operation of the measures forms part of normal day-to-day operations."

From my side I think the security management has to respect and to be designed to follow the business strategy in saving the organizations resources. Or from other side it should be found as a bodyguard of business's process.

3.1.2. The Philosophy from IT Perspective

"Information security management is in which customer business requirements are planned and implemented". [Jacques. A, 1999]

It gave me a feeling that it is just choosing devices and software depending on the customer requirements then implemented. In their model in figure 2 they assigned to a third party "technology provider" to take on this mission by the service level agreement among the provider and the organization, because of that the organization become dependent upon the side of protection. Only the big organization can do that because that costs too much money. Also their model is too complex to be understandable.

In the end here they came out with the code of practice through many years to be ready for use by any kind of organization big or small and new or old these cods with a high probability of risk incident with a different services as "continual service improvement, design, transition, operation and so on", but that from my side goon is a big support to technology providers to manipulate the side of information security.

3.1.3. The Philosophy From Risk Assessment Perspective

Here the philosophy is "to identify, measure, manage, and control the risks to system and data availability, integrity, and confidentiality, and to ensure accountability for system actions" [FFIEC, 2006].

Here the business perspective is missing which can present some strategy's mistake. Also no one can collect 100% of the probabilities of risk incident. For example if some unexpected threats occurs. It will cost money but in future will not cost if it is again done, that, they will implement roles to defeat it.

These points describe three areas of security and business influential or in other definition the area of vulnerability which are “business strategy + threats + information technology “ , also there is other point models I described in last chapter illustrated as a point of top management decision , but it is one area of business influential which is the user’s behavior .

Here I can identify the security management “using rules and tools to secure business’s data depend on business strategy, information technology, and employee from probability of external threat, internal threat and unexpected user’s behavior “

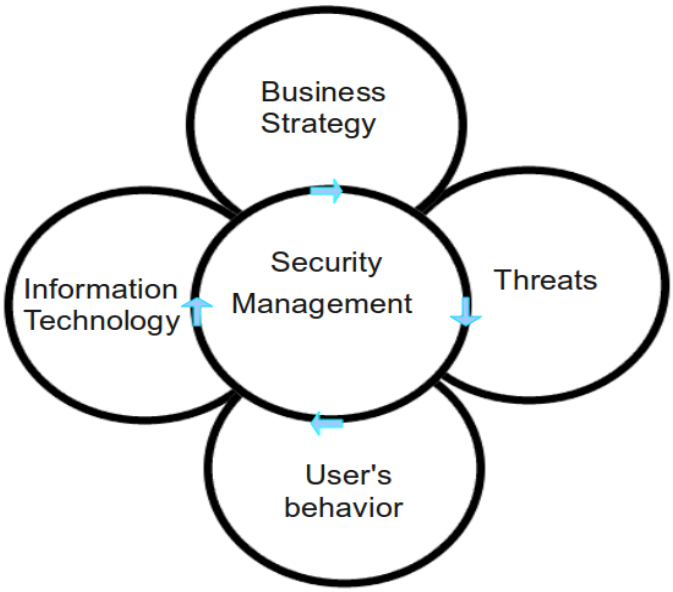

Figure 5 Areas of Protection and Management

3.2. Synthesis

3.2.1. Areas of Vulnerability

Here are definitions of the security areas which were described in last figure (5).

3.2.1.1. Business strategy

Strategy is the direction and scope of an organization over the long-term: which achieves advantage for the organization through its configuration of resources within a challenging environment, to meet the needs of markets and to fulfill stakeholder expectations. Then the Business strategy determine the IT used and, business policy.

3.2.1.2. Information technology

The business sector produces products and services for profit. Information technology describes any technology used to create process and disseminate information that is critical to business performance. Information technology is important to the business sector as a management tool to optimize the processing of information to produce goods and services for profit.

3.2.1.3. Threats

All computers connected to the Internet are at risk in some degree. What risks you face and their severity vary based on what you and your employees do with your PCs. These activities expose you to potential threats and in previous chapter I describe some specific threats.

3.2.1.4. Employee Behavior

Businesses have codes of conduct that are developed to outline expected, and acceptable, standards of employee behaviors. Codes of conduct function as resources for the regulations related to the inner workings of an organization. They are usually provided to employees at the start of employment so that they are aware of what is expected of them from their first day forward.

3.2.1.4.1. Unacceptable employee behavior

Those problem employees who tax even the best managers. And wherever they are, you can be sure they're costing the organization plenty in lowered morale, lost opportunities, and decreased productivity. In fact, the price can be so high that it's foolish to try to overlook or brush aside the problem. If you supervise an employee who has behavior or attitude problems, you need to take action agonist it.

3.2.2. Areas of vulnerability and possible effects of damage

The damage found out because some wrong events, even if inadvertent or advertent and here are most events' Damages.

1. Unauthorized disclosure, modification, or destruction of Information
2. Inadvertent modification or destruction of information
3. Non-delivery or miss-delivery of service

4. Denial or degradation of service

There are three potential consequences in loss of "monetary, productivity and customer confidence sides" occurs depend on the type of damages event and in different levels and next matrix show the probability of damages in three levels.

Next matrix shows the risk level of different area.

Areas of vulnerability and possible effects of damage	Risk of monetary loss			Risk of productivity loss			Risk of loss of customer confidence		
	H	M	L	H	M	L	H	M	L
Employee									
Unauthorized disclosure, modification, or destruction of information			*		*				*
Inadvertent modification or destruction of information	*			*					*
Non-delivery or miss-delivery of service		*				*	*		
Denial or degradation of service	*					*	*		
Information Technology									
Unauthorized disclosure, modification, or destruction of information	*			*					*
Inadvertent modification or destruction of information	*			*					*
Non-delivery or Mis-delivery of service		*				*		*	
Denial or degradation of service			*	*			*		
Business Strategy									
Unauthorized disclosure, modification, or destruction of information	*			*					*
Inadvertent modification or destruction of information	*			*					*
Non-delivery or Mis-delivery of service	*			*				*	
Denial or degradation of service	*			*			*		
Threats									
Unauthorized disclosure, modification, or destruction of information	*				*				*

Inadvertent modification or destruction of information	*			*					*
Non-delivery or Mis-delivery of service	*			*				*	
Denial or degradation of service	*			*			*		
TOTAL	**12**	**2**	**2**	**11**	**2**	**3**	**5**	**3**	**8**

We can calculate the infection level can be in each area as following:

HE is the average of count high infection from employee area

HE $_{(Risk\ of\ monetary\ loss)}$ = 2/4 = .5

HE $_{(Risk\ of\ productivity\ loss)}$ = 1/4 = .25

HE $_{(Risk\ of\ loss\ customer\ confidence)}$ = 2/4 = .5

Here we can see that the risk in monetary loss and loss of customer confidence is higher than in productivity

And the maximum level can be if all the possibility of effecting damages occurred, and here will be the average of all damages type

The average = HE $_{(Risk\ of\ monetary\ loss)}$ /3+ HE $_{(Risk\ of\ productivity\ loss)}$ /3+ HE $_{(Risk\ of\ loss\ customer\ confidence)}$ /3

=1.25/3=.416 => 41%

HI is the count of high infection from information technology area

HI $_{(Risk\ of\ monetary)}$ = 2/4 = .5

HI $_{(Risk\ of\ productivity\ loss)}$ = 3/4 = .75

HI $_{(Risk\ of\ loss\ customer\ confidence)}$ = 1/4 = .25

The average = HI $_{(Risk\ of\ monetary\ loss)}$ /3+ HI $_{(Risk\ of\ productivity\ loss)}$ /3+ HI $_{(Risk\ of\ loss\ customer\ confidence)}$ /3

=1.5/3=.5=>50%

HB is the count of high infection from business strategy area

HB $_{(Risk\ of\ monetary)}$ = 4/4 = 1 => 100 %

HB $_{(Risk\ of\ productivity\ loss)}$ = 4/4 = 1 => 100 %

HB $_{(Risk\ of\ loss\ customer\ confidence)}$ = 1/4 = .25 => 25 %

The average = HI $_{(Risk\ of\ monetary\ loss)}$ /3+ HI $_{(Risk\ of\ productivity\ loss)}$ /3+ HI $_{(Risk\ of\ loss\ customer\ confidence)}$ /3

=2.25/3=.75=>75%

HT is the count of high infection from threat area

HT $_{(Risk\ of\ monetary)}$ = 4/4 = 1 => 100 %

HT $_{(Risk\ of\ productivity\ loss)}$ = 3/4 = .75 => 75 %

HT $_{(Risk\ of\ loss\ customer\ confidence)}$ = 1/4 = .25 => 50 %

The average = HI $_{(Risk\ of\ monetary\ loss)}$ /3+ HI $_{(Risk\ of\ productivity\ loss)}$ /3+ HI $_{(Risk\ of\ loss\ customer\ confidence)}$ /3

=1.97/3=.65=>65%

3.2.3. DLC and Security Management Process

We know business no longer deals in documents. It deals in "data." And data is given life to the business and that life starts with collecting data which has a value to business, then creating plan of producing service or product, and processing the plan created by implement it under control and auditing for maintain it, in the end saving the required data. These processes will be repeated more and more till the data lose its value to the organization.

If we consider the security management process is a service needed to be produced or in other side to be understandable as the end product then implement data life cycle management, we will get the following process:

Collecting security data required >creating security plan covering all probability of risk incident >processing security plan within action > storage data needed for future

3.2.3.1. Targeted Data

As I describe before and from the last matrix any infection in any area can cost money. Because of that I will find out each data can be collected in each area:

- Data of business strategic in (production process, responsibility of data process, customer types and communication also delivery rules)
- Data of information technology is in what technical used in “production, communication among branches departments and customer “
- Data of threats in the possibility of risk incident and it is level and effective on the organizations business

- Data of employee in management structure and responsibility

3.2.3.2. The Plan

The plan should cover all the possibility of risk incident through building conditions and laws and rules to control the user's behavior in production line.

And creating the statement of policies agreed with the top management to determine responsibility of each employee.

Creating the statement of devices and software you have and you need to add or change to achieve the security level requested.

Creating the training plan to increase the employee knowledge of using technology in safe mode

3.2.3.3. The Plan In Action

To achieve the plan you have to put it in action to be in real lives which start with implement the plan by installing the devices and the software of production and. And teaching the staff how to deal with the new technology and remaining each employee with his responsibility.

Evaluate all that through controlling and auditing the working life and putting the notes that will improve the implementation or make a change in the plan implemented

3.2.4. The Summary

There are many areas related to the security management each area has its effect in the organization business by positive or negative here these areas are in threats, business strategy, information technology and the users behavior.

I used the data life cycle in the four area described to find out the security management process , and by the process of data life cycle which in collect, create, process and storage

I came out with the model described in next chapter.

4. Method Description

Here, in this chapter I am going to analyze and design of security management on base of DLC. Information life cycle management enables us to understand our data, which is an extremely valuable business asset and which must be managed properly, to ensure business success and regulatory compliance... And Understanding data management is meaning classify and determine rules, responsibility and IT needed and determine the security policy's requirement.

Each stage in life cycle should be done by human through technology follows the business strategy; avoiding risk occurs. The following figure shows my method which I will display in this chapter

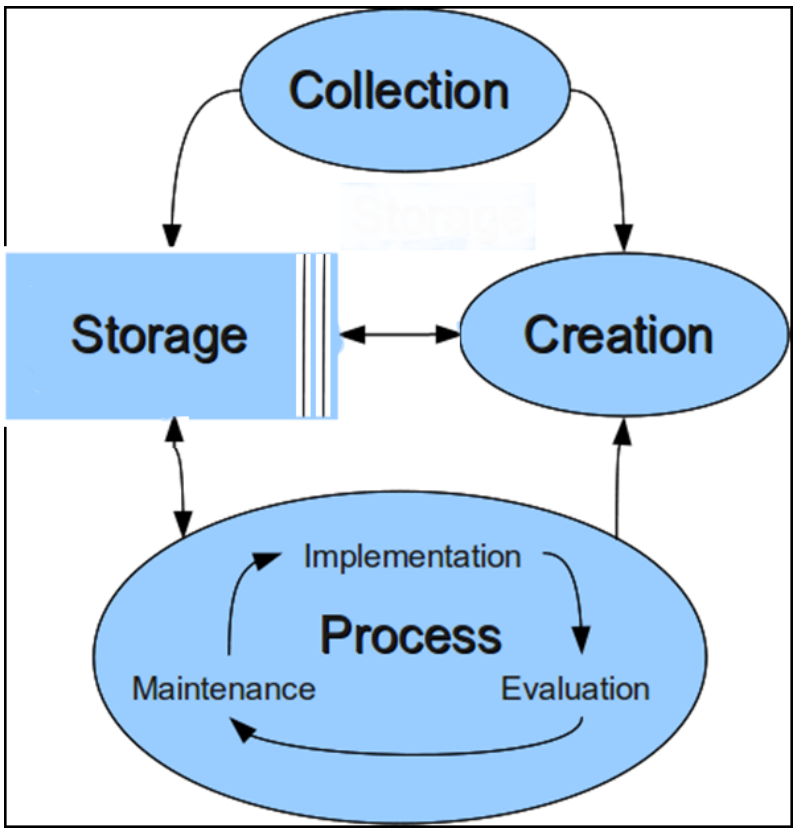

Figure 6 Security Management Process from DLC Perspective

It is a collection of some activities which have to be followed to achieve the organization's security; also as we will see each activity has sub process ends with reports collected in basket work to be used in other activities to build the organization

security base. The following table includes the activity with simple identification and description:

Table 3 Process Activities and Definitions

Activity	Description
Collection	Include sub-process to collect different information and ends with reports
Creation	Include also sub-process to made plans and ends also with specific reports
Process	Also sub process to implement and evaluate and maintain also ends with specific reports

4.1. Collection Process

This activity include sub process in, Finding out specific organization management structure, outline the scenario of business's process and find out probabilities of threats and vulnerabilities of occurrence and outcomes, which can be done through constructing team work from three experts and their duty are to consulting the responsible people from the organization to discuss and collect displayed request, and this process ends with specific reports which have a value.

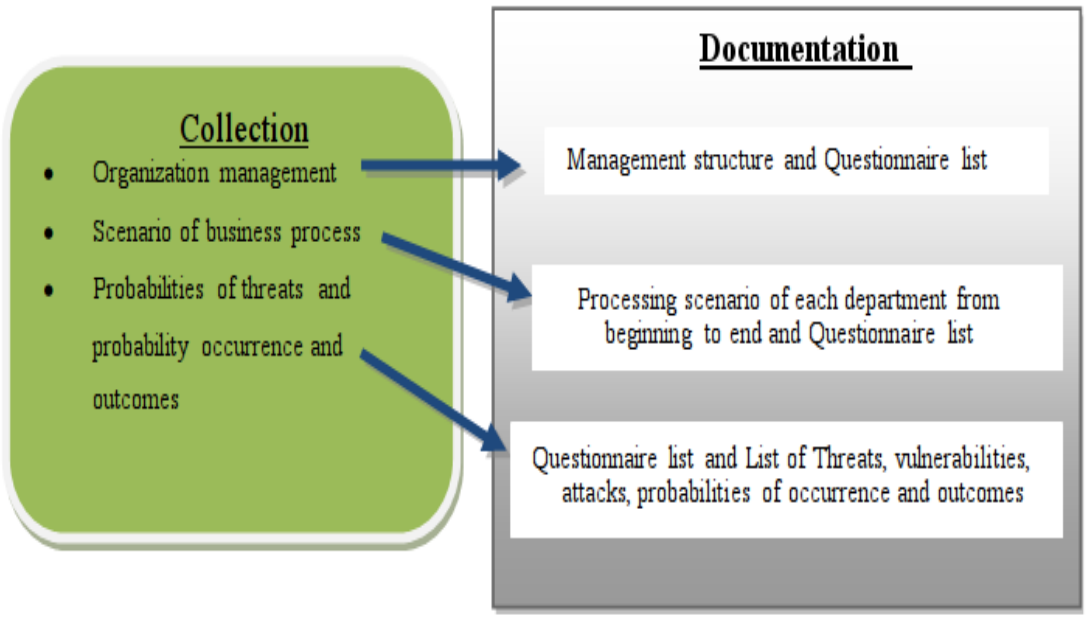

Figure 7 Collection Process and its Results

4.1.1. Organization Management

In this process the expert will meet and consult the top manager and the department's managers of the organization about the relation between the top manager and the department also the relation between the department's managers and their employee, then formulate the data in graphical way.

Either they have to prepare a Questionnaire related to security management that the managers have to answer.

That to get information about security management situation, identity management, security policy and change security management in organization, Look for questions which can be in the questioners possible in the appendix stage no-A data no 5.

4.1.2. Scenario of Business Process

In this process the expert will flow the organization's data process of production from the beginning to ends and register each change on data and by what and who, in the end he has to formulate the scenario diagram by using any case tools for example UML. That will give information about tools and rules used to create goods or services, from technical used hardware and software also shows communication from inside and outside the organization.

Also as before have to prepare a Questionnaire related to employee security focus and event management security. Look for the example in appendix stage no-A data no 5.

4.1.3. Threats and Probability Occurrence and Outcomes

The expert should analyze through scenarios the probability of different threat agents causing damage. These scenarios should consider the organization's business strategy, quality of its control environment, and its own experience, or the experience of other institutions and entities, with respect to information security failures.

The assignment of probabilities by the organization should be appropriate for the size and complexity of the institution. Simple approaches (e.g., probable, highly possible, Possible, and unlikely) are generally sufficient for smaller, non-complex institutions.

The expert prepares two kinds of Questionnaires for employee and managers, one related to application security, network security and system security.

And the second to determine the level through the most four damages type can occur in Areas of vulnerability (Personnel, Facilities and equipment, Applications, Communications, Software and operating systems):

- Unauthorized disclosure, modification, or destruction of information
- Inadvertent modification or destruction of information
- Non-delivery or miss-delivery of service
- Denial or degradation of service

Look for the appendix stage no-A data no 5.

4.2. Creation Process

As before this activity has sub process to outlines the specific requirements and rules that have to be met in order to implement security management and ends with a policy statement also determine the technical requirements from soft and hard and The general formulated goals are specified in operational level agreements. These agreements can be seen as security Plans for specific organization units. Next figure show the sub-process and the reports outline.

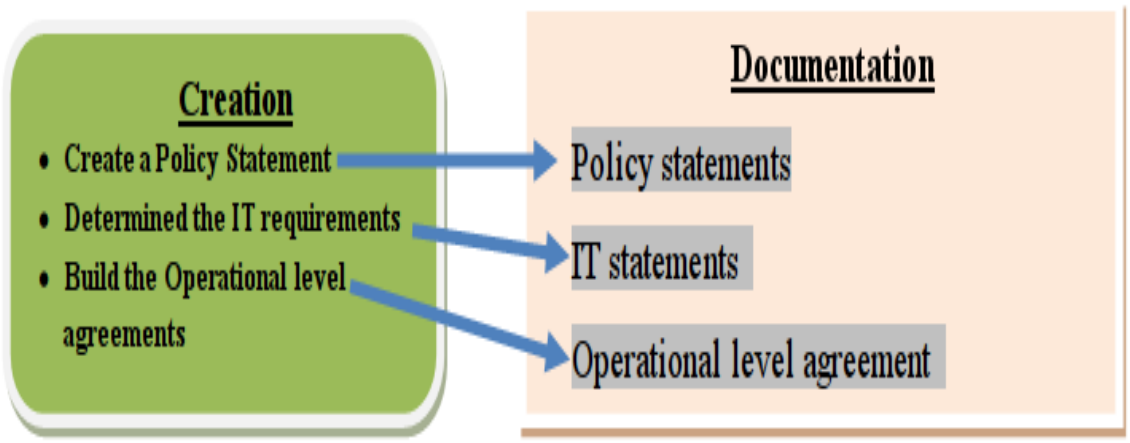

Figure 8 Creation Process and its Results

4.3. Processes

The process activity has three sub activities implementation, evaluation and maintenance of the plan created in last stage in the operational agreement. Next table include a description of the process activity.

Table 4 description of the process activity (author)

Activities	Sub-Activities	Descriptions
process	Implementation	This process to put the operational agreement in action.
	evaluation	This process to audit and control the result of action to evaluate the security level
	Maintenance	This point to reconstruct and create the operational plan

4.3.1. Implementation

In this process there are sub process summarized in classifying and managing applications, implement personal security, security management, access control and reporting.

- classifying and managing applications

  Process of formally grouping configuration items by type, software, hardware, documentation, environment, application Process of formally identifying changes by type e.g., project scope change request, validation change request, infrastructure change request this process leads to asset classification and control documents.

- implement personal security

  Here measures are adopted in order to give personnel safety and confidence and measures to prevent a crime/fraud. The process ends with personnel security.

- security management

  In this process specific security requirements and/or security rules that must be met are outlined and documented. The process ends with security policies.

- access control

In this process specific access security requirements and/or access security rules that must be met are outlined and documented. The process ends with access control.

The following shows that activity ends with documents

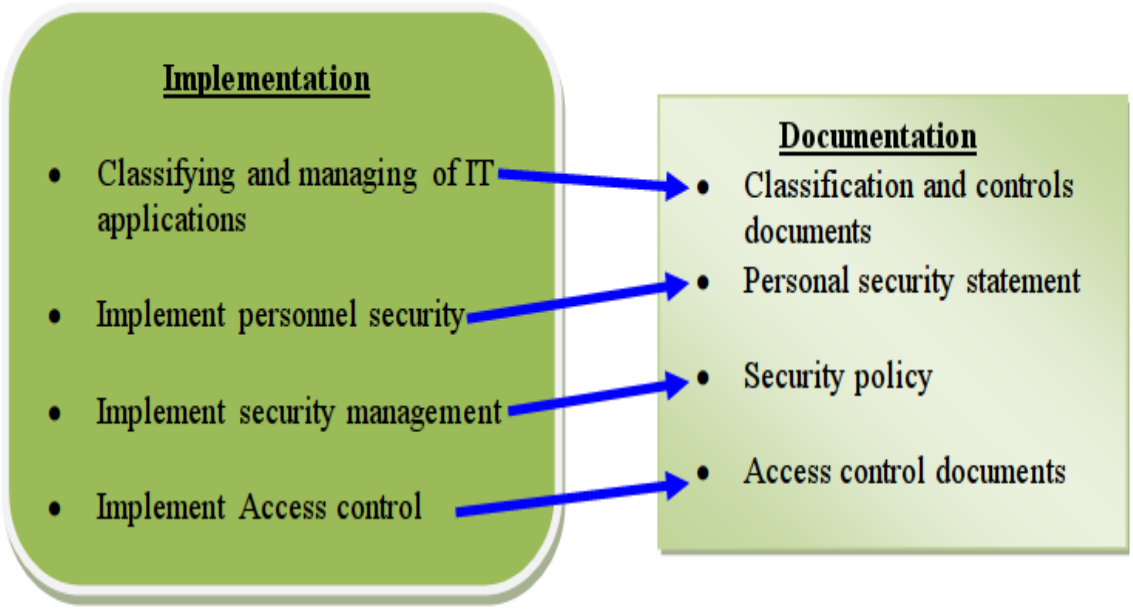

Figure 9 Implementation Process and Results

4.3.2. Evaluation

In this process starts with examination of the implemented processes by a sub-process in:

- Self assessments.

In this process an examination of the implemented security agreements is done by the organization of the process itself. The result of this process is self assessments documents.

- Internal Audit.

In this process an examination of the implemented security agreements is done by an internal Electronic Data Process EDP auditor. The result of this process is Internal Audit statement.

- External audit

In this process an examination of the implemented security agreements is done by an external Electronic Data Process EDP auditor. The result of this process is External audit statement.

- Evaluation based on security incidents

In this process an examination of the implemented security agreements is done based on security events which is not part of the standard operation of a service and which causes, or may cause, an interruption to, or a reduction in, the quality of that service. The result of this process is security incident reports.

And here is the figure illustrates that:

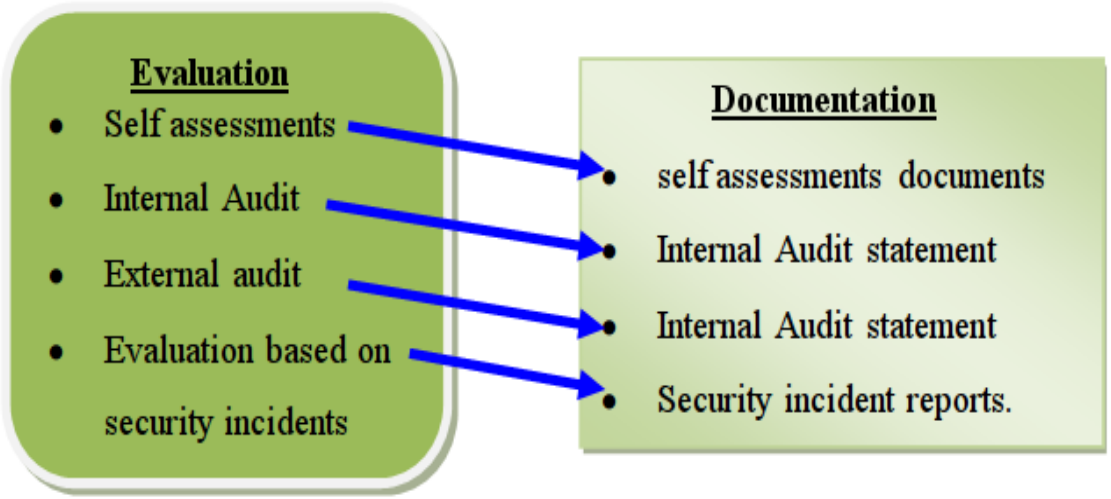

Figure 10 Evaluation Processes with Results

4.3.3. Maintenance

As before there are sub processes to improve the implemented processes to cover any problem came out and these process are:

- Maintenance of Service level agreements

This process to keep the service level agreements in proper condition, and ends with Maintained Service level agreements

- Request for change to OLA

Request for a change to the OLA is formulated. This process ends with a request for change

- Reports

In this process the whole maintain implemented security policies process is documented in a specific way. This process ends with REPORTS.

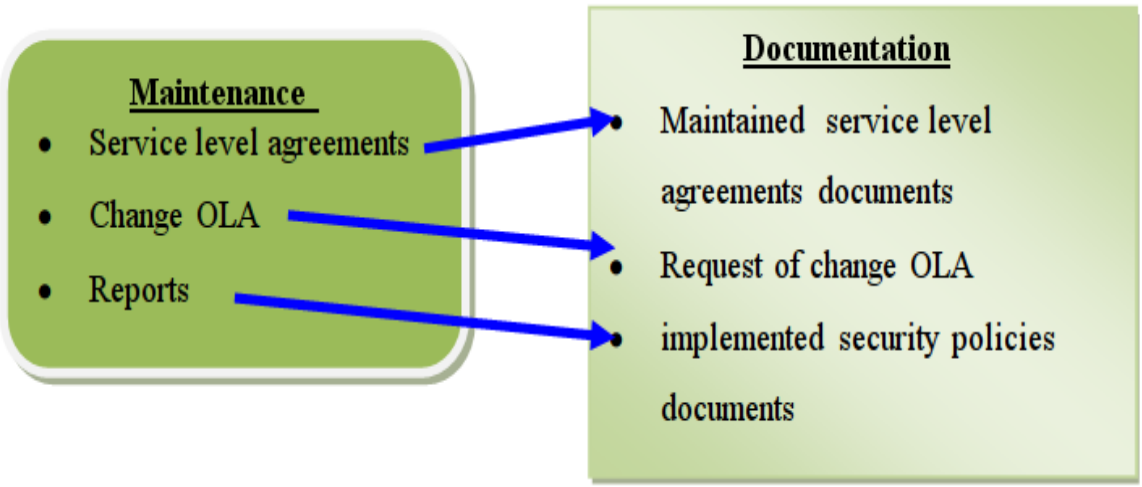

Figure 11 Maintenance Process and its Results

4.4. Storage Unit

Storage process is to create and maintain the basket work which will be the base of the security management data and security operational level change.

This process exists in all security management stages through collecting documents resulted by processes and redistribute again to maintain and improve the processes as the following figure show the management process and the documentary system in storage process.

Each document has specific way to display processes result look for the appendix c where exist some examples of resulted process.

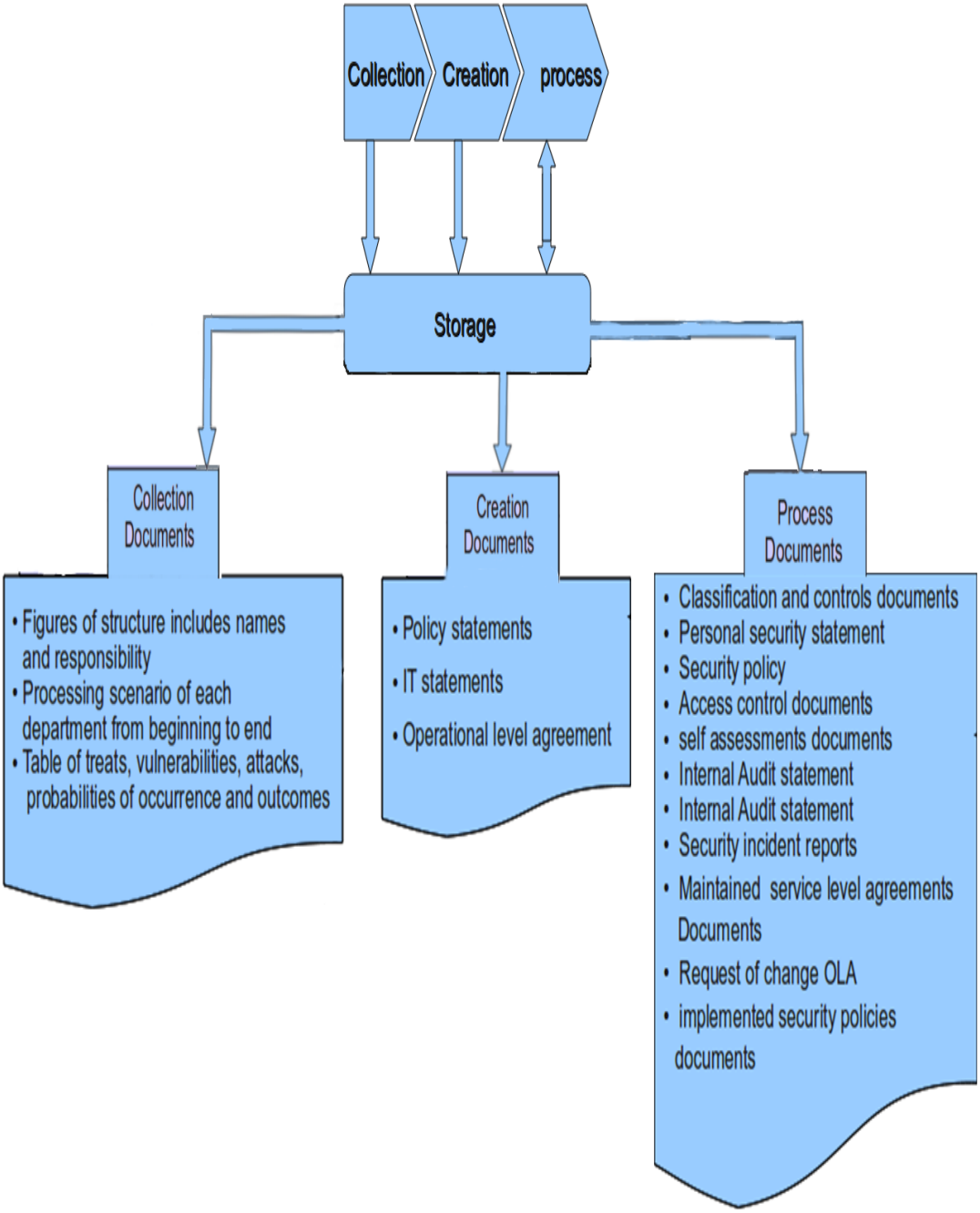

Figure 12 Storage Unit and Documentation

4.5. Summary

I can summarize my model in four steps: first collecting data required through analyzing the existing system's situation to find out three things (the management structure, the processing scenario in the organization and the threats vulnerabilities and probabilities of occurrences). Second creating the security plan which includes (policy statement the determination of responsibility, IT statement the determination of IT required and the operational level agreement which considered the security policy) depend on data collected.

The 3D is including three activates of implement, evaluate and maintain the created plan. The 4th is the basket work where all data has to be saved. That was my model of management security which can be implemented in any kind of organization and in next chapters I will try to prove my model by implement it in Libya insurance company as chosen company, in next chapter will be more details about this company.

5. Environment of Implementation

5.1. Libyan economic overview

The Libyan economy depends primarily upon revenues from the oil sector, which constitute practically all export earnings and about one-quarter of gross domestic product (GDP). In the early 1980s, Libya was one of the wealthiest countries in the world; its GNP per capital was higher than that of countries such as Italy, Singapore, South Korea, Spain and New Zealand.

Today, high oil revenues and a small population give Libya one of the highest GDPs per person in Africa and have allowed the Libyan state to provide an extensive level of social security, particularly in the fields of housing and education.

Many problems still beset Libya's economy however; unemployment is the highest in the region at 21% according to the latest census figures.

Compared to its neighbors', Libya enjoys a low level of both absolute and relative poverty. Libyan officials in the past three years have carried out economic reforms as part of a broader campaign to reintegrate the country into the global capitalist economy.

This effort picked up steam after UN sanctions were lifted in September 2003, and as Libya announced in December 2003 that it would abandon programs to build weapons of mass destruction.

Libya has begun some market-oriented reforms. Initial steps have included applying for membership of the World Trade Organization, reducing subsidies, and announcing plans for privatization.

The non-oil manufacturing and construction sectors, which account for about 20% of GDP, have expanded from processing mostly agricultural products to include the production of petrochemicals, iron, steel and aluminum. [CIA, 2010]

Climatic conditions and poor soils severely limit agricultural output, and Libya imports about 75% of its food. Water is also a problem, with some 28% of the population not having access to safe drinking water in 2000.

The Great Man-made River project is tapping into vast underground aquifers of fresh water discovered during the quest for oil, and is intended to improve the country's agricultural output.

Under the previous Prime Minister, Shukri Ghanem, and current prime minister Baghdadi Mahmud, Libya is undergoing a business boom. Many government-run industries are being privatized.

Many international oil companies have returned to the country, including oil giants Shell and ExxonMobil Tourism is on the rise, bringing increased demand for hotel accommodation and for capacity at airports such as Tripoli International.

A multi-million dollar renovation of Libyan airports has recently been approved by the government to help meet such demands. At present 130,000 people visit the country annually; the Libyan government hopes to increase this figure to 10,000,000 tourists.

Saif al-Islam al-Gaddafi, the oldest son of Muammar al-Gaddafi, is involved in a green development project called the Green Mountain Sustainable Development Area, which seeks to bring tourism to Cyrene and to preserve Greek ruins in the area.

5.2. Libya insurance company

5.2.1. History and Overview

During the med of the sixties, the government planned to establish a public insurance company. To prepare for competition, the royal group, London & Lancashire, and Union joined together in establishing a company under the name of (North Africa).

The Eagle star established a company with the name of (the Sahara) while Egypt Insurance registered as (Al Mukhtar). Even some Libyans had shares in those companies, very rare Libyans engaged in the staff.

On 1/9/1969 Al Fatah revolution came to power and took immediately many procedures concerning insurance in order to protect the national interest.

The first was to illegalize All insurance activities accept for insurance companies registered in Libya, the second was the issue of 131/1970 act concerning supervision and control of insurance companies on 26/10/1970 and in the same year, the 156/1970 act was issued.

The 156/1970 act nationalized all foreign shares in all insurance companies registered in Libya. Compensations were fully paid. On 28/12/1980 the General Popular Committee issued an enactment by which Al Mukhtar Insurance Company was merged in Libya Insurance Company.

The purpose was to:

1- Increase the financial and capacity ability.
2- Avoiding negative effects of competition.
3- Re-organizing insurance activities according to political views of the country.

As a result, Libya Insurance Company increased its capital to LD30, 000,000.Libya Insurance Company became the only insurance company in the market till 1998.

On 12/1/2005 the 3/1374-2005 act concerning the supervision and control of insurance activities, was issued. By this new act, the 131/1970 act and 156/1970 act were canceled. The act permits and clearly allows private sector to invest in insurance.

During 2005 permissions were given to establish more private insurance companies. And there are five direct insurance companies competing in the market. [LIC, 2005]

5.2.2. Organization structure

Libya insurance company consists of “top management “represents as the people committee”, main branch “is the branch which supervision and control the whole company” and 7 branches distributed in Libya to offer the company’s service to all citizens.

Following illustrative shows the structure of LIC including departments in both of main branch and people committee.

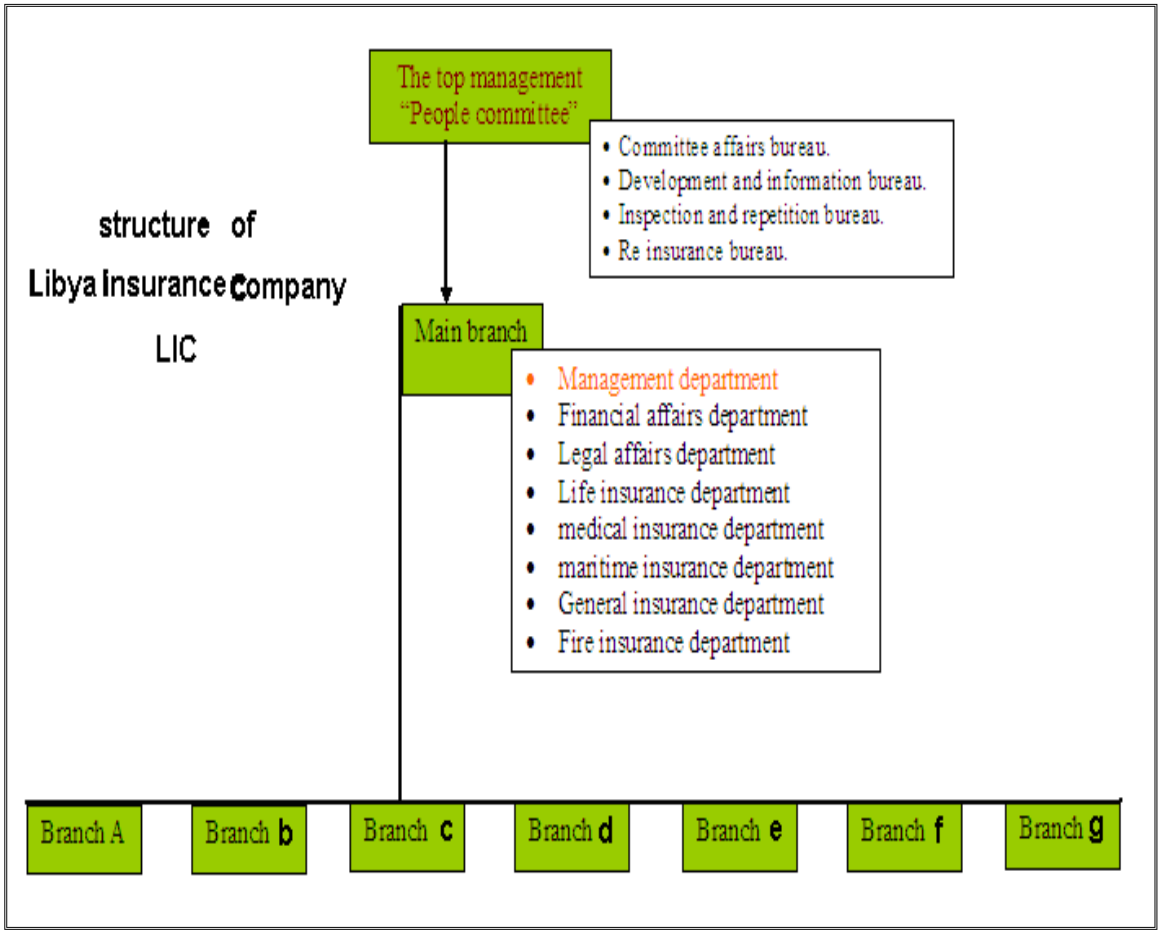

Figure 13 Libya Insurance Company Structure

5.2.3. Choice of insurance product

From the consultation and the discussion with the top manager and my reading of the Productivity, Technology and Economic Growth of [Bart Van Ark, 2000] and the internal company's journals he gave me [LIC, 2005], I can describe this task of productivity as following:

4.1.1.1.Cargo Insurance

Cargo insurance (also called marine cargo insurance) covers physical damage to or loss of your goods whilst in transit by land, sea and air and offers considerable opportunities and cost advantages if managed correctly.

Here are the covered cargo categories

4.1.1.1.1. Institute cargo clauses for goods transported by sea.

4.1.1.1.2. Institute cargo clauses for goods transported by air.

4.1.1.1.3. Inland cargo insurance for goods transported in land.

4.1.1.1.4. Bulk Oil Insurance.

4.1.1.2.Marine Hull Insurance

Marine Hull Insurance covers loss or damage to hull and machinery. The hull is the structure of the vessel. Machinery is the equipment that generates the power to move the vessel and control the lighting and temperature system such as boiler, engine, cooler and electricity generator. And it's category as following:

4.1.1.2.1. Institute Fishing vessels clauses.

4.1.1.2.2. Institute Hull and Machinery clauses.

4.1.1.2.3. Institute port risks clauses.

4.1.1.2.4. Stevedore's liabilities.

4.1.1.2.5. Personal Accident for Mariners.

4.1.1.3.Aviation Insurance

Aviation insurance is insurance which is designed specifically to meet the needs of aviators. There are a number of different types of available for a variety of aircrafts and pilots. Laws about aviation insurance tend to be less clearly defined than those regarding car insurance, which can make it difficult to choose the right policy and carrier. Pilots who are not familiar with the specifics of the industry may want to consider asking for advice from an insurance broker or an experienced pilot.

Just as with insurance for other types of vehicles, there are a number of levels of coverage in aviation insurance policies, including liability coverage for accidents when the policyholder is at fault, theft and loss coverage, life insurance riders, and insurance for other types of situations, such as loss of cargo. The more services requested on a policy, the more expensive it will be. Coverage also varies depending on the type of craft: helicopters, sport planes, commercial airliners, and so forth are all covered differently.

4.1.1.3.1. Plane Hull.

4.1.1.3.2. Liabilities of Air Carrier

4.1.1.3.3. Pilot and Crew Personal Accident.

4.1.1.3.4. Loss of Licenses.

4.1.1.4.Fire Insurance

Fire insurance is a form of property insurance which protects people from the costs incurred by fires. When a structure is covered by fire insurance, the insurance policy will pay out in the event that the structure is damaged or destroyed by fire. Some standard property insurance policies include fire insurance in their coverage, while in other cases; fire insurance may need to be purchased separately. Property owners should check with their insurance companies if they are not sure whether or not fire insurance is part of their policies, and if fire insurance is not included, it should be purchased.

4.1.1.4.1. Fire, Lightening, and additional Risks.

4.1.1.4.2. Burglary.

4.1.1.4.3. Energy and Petroleum Risks.

4.1.1.4.4. Off Shore Drilling Rigs.

4.1.1.4.5. Family Protection Insurance.

4.1.1.5.Motor Insurance

4.1.1.5.1. Compulsory Insurance.

4.1.1.5.2. Private Vehicle Comprehensive.

4.1.1.5.3. Commercial Vehicle Comprehensive.

4.1.1.5.4. Third Party liability, Fire and Theft.

4.1.1.5.5. Arab Card.

4.1.1.5.6. Green Cards

4.1.1.6.Health insurance

From time to time, one of your loved ones may become ill or be involved in an accident. This could be a very costly experience that would put your family's financial well being at risk. LIC insurance offers a variety of health insurance policies that may help you prevent future financial loss in case of an accident, illness, hospitalization or surgery.

4.1.1.7.Miscellaneous Insurance

4.1.1.7.1. Cash In Transit.

4.1.1.7.2. Cash In Safe.

4.1.1.7.3. Fidelity Guarantee.

4.1.1.7.4. Personal Accident.

4.1.1.7.5. Bankers' Policy.

4.1.1.8.Liabilities Insurance

There are many different types of insurance policies available, but liability insurance is one of the most popular because it costs much less than many other options. For example, in regard to auto insurance policies, liability insurance costs far less than full coverage. The reason for this is because full coverage insurance must pay for both your vehicle and any other vehicle involved in a collision, as well as property damage and medical expenses due to injuries to you or another party.

On the other hand, liability insurance is only responsible for the other party's losses. Your person and your property are unprotected, but liability insurance protects you from being held responsible for the other party's damages.

There are different types of liability insurance

4.1.1.8.1. Employer's Liability.

4.1.1.8.2. Civil Liability.

4.1.1.8.3. Medical Liability.

4.1.1.8.4. Product Liability.

4.1.1.8.5. Professional Liability.

4.1.1.9.Life insurance

4.1.1.9.1. Whole Life insurance

Whole life insurance is permanent life insurance protection that protects your family or business no matter what lies ahead, from the day you purchase the policy until you die, as long as you pay the premiums when due.

Whole life insurance can be a solid foundation upon which to build a long-term financial strategy because it guarantees a lifetime of protection for your family or business.

4.1.1.9.2. Term Life insurance.

Term Life Insurance is the simplest form of life insurance. It provides affordable protection for a specific period of time at a scheduled premium level. Premiums may increase at the end of the term.

You choose a coverage level, a term (usually 5, 10, 15, or 20 years) and name a beneficiary, that is, the person you want to receive the benefit if you die. If you die while your term life insurance policy is in force, the death benefit is paid to the beneficiary you chose.

At the end of the term, you can renew your coverage often at a higher premium, without having to provide evidence of good health. You can also convert it to a permanent life insurance policy which builds cash value and may earn dividends.

5.3. Information Technology and Communication in Libya

Libya has not been late in catching up with the developments in the IT sector. Unlike the rest of the Maghreb countries though, Libya's ITC related policies are quite different. Libya's ITC sector has remained for a long time under the monopoly of the public-sector companies. Since 2005, Libya has scaled up investments in the telecoms sector.

Economist Intelligence Unit (EIU) reported in its 2006 bulletin that there were 750,000 fixed telephone lines in Libya in 2005, i.e. fixed-line telephones represented 14 percent.

There were also 234,000 mobile subscribers in 2004, the equivalent of 4 percent coverage of Libya's total area.

Both the fixed and mobile telephony networks are controlled by the state through the public Postal and Telecom Authority and the state- owned GSM operator Almadar. The GSM tariffs levied by Libya's only GSM operator then remained one of the highest in the North African region until 2004.

The entry of a new GSM mobile service provider in September 2004 was positive for the Libyan GSM market. In a short period, the number of mobile phone subscribers jumped to 500,000. Libya is expected to have 2.5 million mobile subscribers in 2008 if demand maintains the same pace. Only after a short period, since the new Libyan GSM service operator started operation, the Libyan state-controlled telecommunication company initiated a major investment to modernize the public telephone network.

The Libyan public telecom corporations stroke a EURO 200-million deal with Alcatel of France and Nokia of Finland. The deal aimed at expanding the mobile telephony network and reached a target of 2.5 million new subscribers. In 2005, it concluded a EURO 58 million deal with Ericsson of Sweden for the acquisition of a global system for mobile communication technology.

Despite the progress recently achieved by the Libyan telecommunication sector, several challenges continue to impede the emergence of a well-developed and robust telecommunication sector in the country. Any real development of the telecom sector will

require the availability of highly qualified IT specialists that neither the Postal and Telecom Authority nor Almadar GSM operator can develop. [ITC, 2006]

The Internet service was introduced in Libya in 1999 as one of the value -added services to the fixed line telephone service. As of 2004 Libya had 205,000 Internet users.

Access to the internet remains very low compared with the good fixed and mobile telephony access. This low fraction of household subscription may explain the presence of a big number of Internet coffees in the Libyan cities and the high number of users frequenting them, mostly young people.

The ITC sector in Libya needs a set of measures to achieve a real and across the board development. Libya needs to setup an independent LTC authority that will lead the country's efforts to create a knowledge based society. The remit of this authority will include the formulation of plans and policies to generalize the use of ITC technologies in all sectors of the economy.

Performance and productivity of Libya's state firms need to be rated and evaluated in compliance with recognized industry international standards in order to spot shortfalls and recommend corrective measure. On the regulatory front, Libya needs to set up an independent panel to regulate the ITC sector. [ITC, 2006]

The telecom sector should also open the door for local and foreign investments to ensure a competitive and vibrant telecom sector. Local-private sector companies should also be encouraged to form joint ventures with state's public companies to minimize the administrative bureaucracy in one of the fastest growing sectors of the economy.

Libya should also work harder to adopt the international standards recommended by the World Trade Organization (WTO) to be able to get a favorable treatment within the framework of the international cooperation related to the transfer of advanced technologies. Such programmer will allow Libyan nationals to develop their skills and expertise in all ITC disciplines. Within the same context, Libya should seriously explore all the possible schemes to invest in the ITC-related education. PCs and IT related technologies should be made available in all Libyan secondary schools and institutes.

The state should also consider splitting the Postal and Telecom Authority into two autonomous entities to give a boost to both sectors.

New forms of partnership with the private sector companies should be explored in order to raise performance and competitiveness. [ITC, 2006]

5.3.1. Libya for technical and Communication Company LTC

It is a public company and the responsible of communication and technology. Established in year 1997 when started to studying and searching to put the first block of Internet service provider and in year 1999 in the beginning of September started its project to become the main of Internet providers in Libya. [ITC, 2007]

Service growth

- In year 1999 started the commercial telephone dial-up service.
- In year 2001 started their service with to kind "privet telecommunication signal and DSL lines "that was to offer an unlimited fast lines, both services special for the publication organizations.
- In 2005 started to distribute ADSL service to provide fast connection to users at their resident.
- In the same year started the public registration domain ccTLD.
- Also started the Internet satellite service (DVB-RCS).

Future planned

- Libyan WIFI and WIMAX

  Started the company through this year, publishing the WIFI service to cover determined places as airports, coffees, and the general public places, also conferences and exhibitions.

  And now the company managing project to provide the newsiest technical services, "WI MAX", which help to distribute the intent on mobiles and PDA devices .The company going to expansion to cover all country by ADCL, DVB-RCS services

5.3.2. Libya Insurance Company and IT

Evidenced Libya insurance company during last year's a rise in size of business, which made a big coil in procedure of process and that returned to the technical shortage, where operations prepared handily with primary tools, that caused by UN Sanction on the Libyan technical imports.

LIC understand that there problems solution is in technology, that was clear noted, After UN Sanction over where was the company activity foxed in ability of entering technology to their business.

Also the government was putting it in their primary action increasing technology in all lives domain and started by taking taxes on technology over, to support and help people and company to increasing the acknowledgment and skills.

From that side the company implements information technologies in all branches to follows the technology progress with their minimum knowledge of implementing and manage security. That was the point of my chosen of implementation my method (Company with new technology lack the minimum knowledge of the protection and management data).

6. Method Implementation

Information technology considered as sword with two faces, one face is the correct in use and the other face is the wrong in use. Which means it can be used to find good by legal way, also it can be used with illegal way to find good or to shut-down the others or the competitor. That brings up other revolution of technology which related to secure data and recourses of organization.

The more important point in secure data is to understand the tools of risk incident. In the other describe is the acknowledgement of risk occurs. To know how the damage occurs and whose did and what he did to get the damage, that damage can be internal or external, internal can occurred by employee and the external occurred by person not related to the organization to get in the organization's recourses for one of two things to do Destroying or Copying the contents.

The important things must be done to applying security rolls is determine the security equipment by playing a quality system analyze.

Here I will describe and analyze the situation in the organization from view of information security flowing the data life cycle.

6.1. Existing System analyze

As I said in the last chapter the company is to big because of that I will focus in my work in the main branch.

6.1.1. Management structure in Tripoli branch

In this part I was consulting managers (the top manager and the branches managers) that to get clear view of the management structure and I found that:

In Libya insurance company each branch become look like a small privet organization, includes a technical devices, users, customers, and data which corporate together to give service to customer and profit to company, just the general strategy will guide with the top management "people committee".

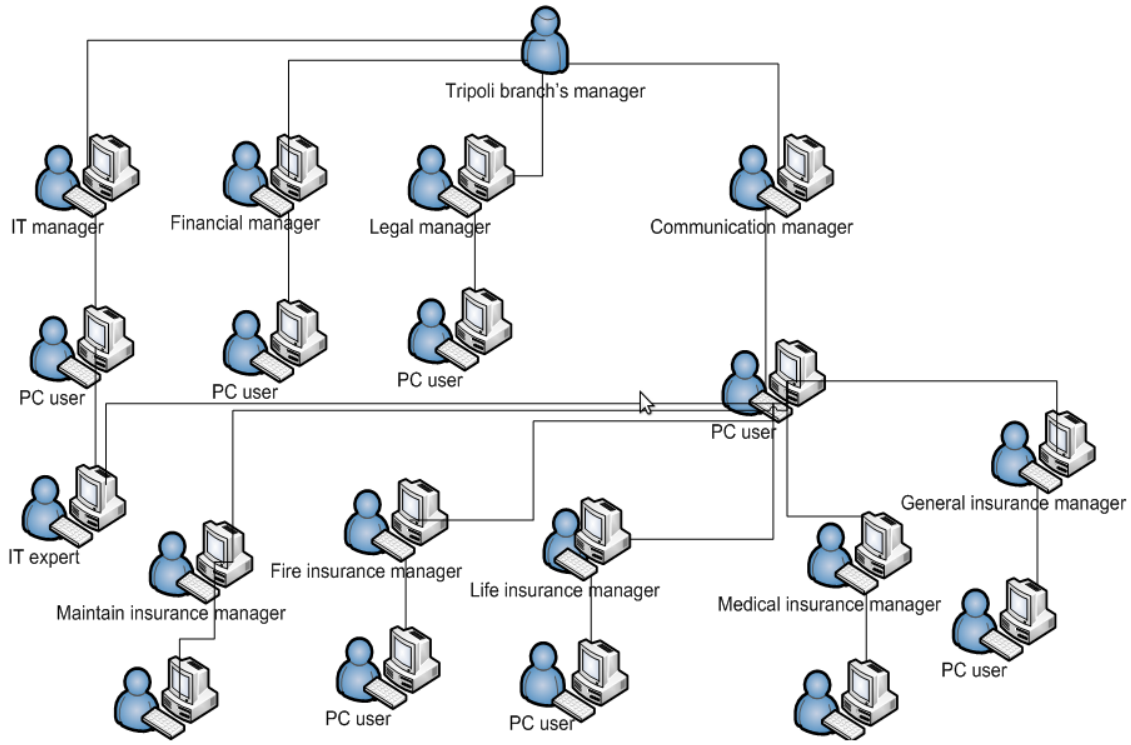

Figure 14 Management Structure of Tripoli Branch

In Tripoli branch of LIC- there are 9 departments each department has usually 2 processors technically and one PC expert user, in figure 14 described the tree structure of Tripoli management. Where Departments of maintain, medical, life, fire and general insurance will come after the manager of the communication department which consider also the bridge between all branches and the manager of Tripoli branch, but the other connected directly to the branch manager, the figure 15 show the interface system in Tripoli branch of LIC.

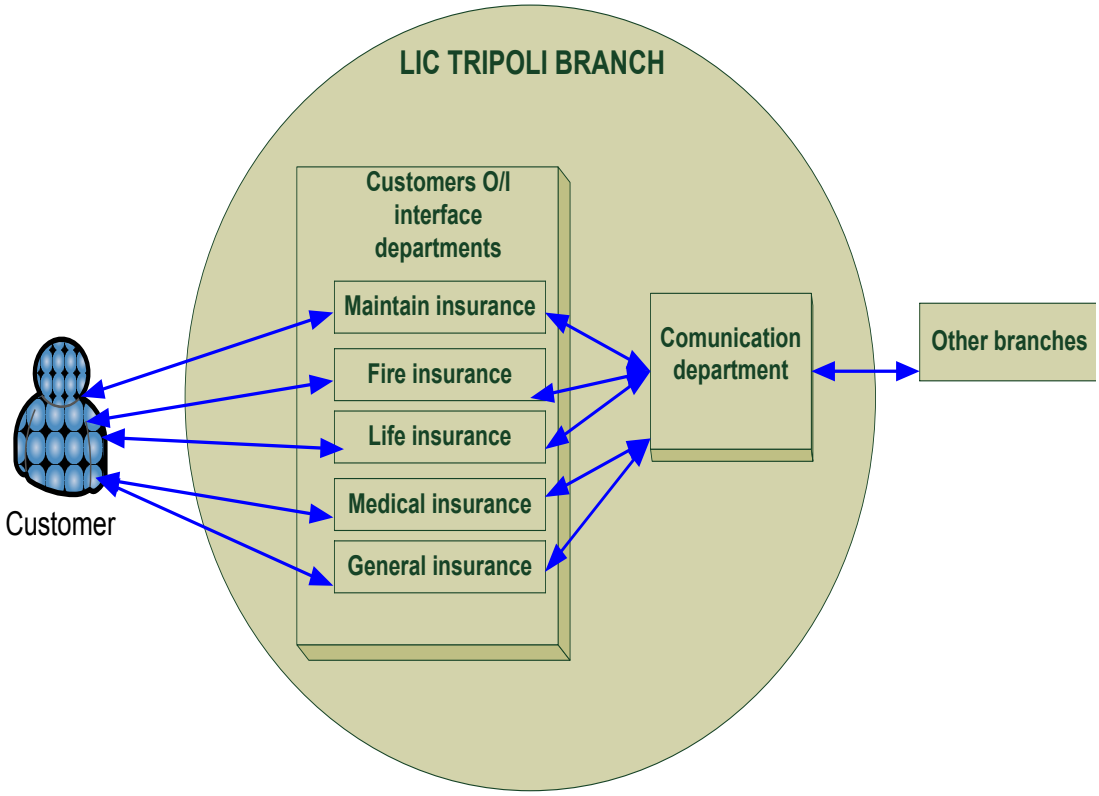

Figure 15 Interface System in Tripoli Branch

In this process I discussed with the PC-user about his duty and I found out:
Each branch has to deal with a different data, using the same procedure and offering different service's type to the customers.

With respect of company's targets and policies of general strategy, branches have to deal with Data as a privet organization, and decision making of creating, analyzing, processing and keeping or deleting data.

There is no different in the branch's target and size, they are proximately similar, only Tripoli's branch has a difference. This difference caused by centralizing database in it, to become a center of communication in company, which I described before.

The following diagram is the actual system structure in one department of the main branch of Libya insurance company with employing Information Technology on the business, which will show the frame system of data life cycle inside whole

the company. That as I describe before, “all departments have the same roles and processing scenario, and if you understand one you understand all departments”

In this diagram there are two kind of processors, users and technical devices, cooperate together to achieve a customer satisfaction.

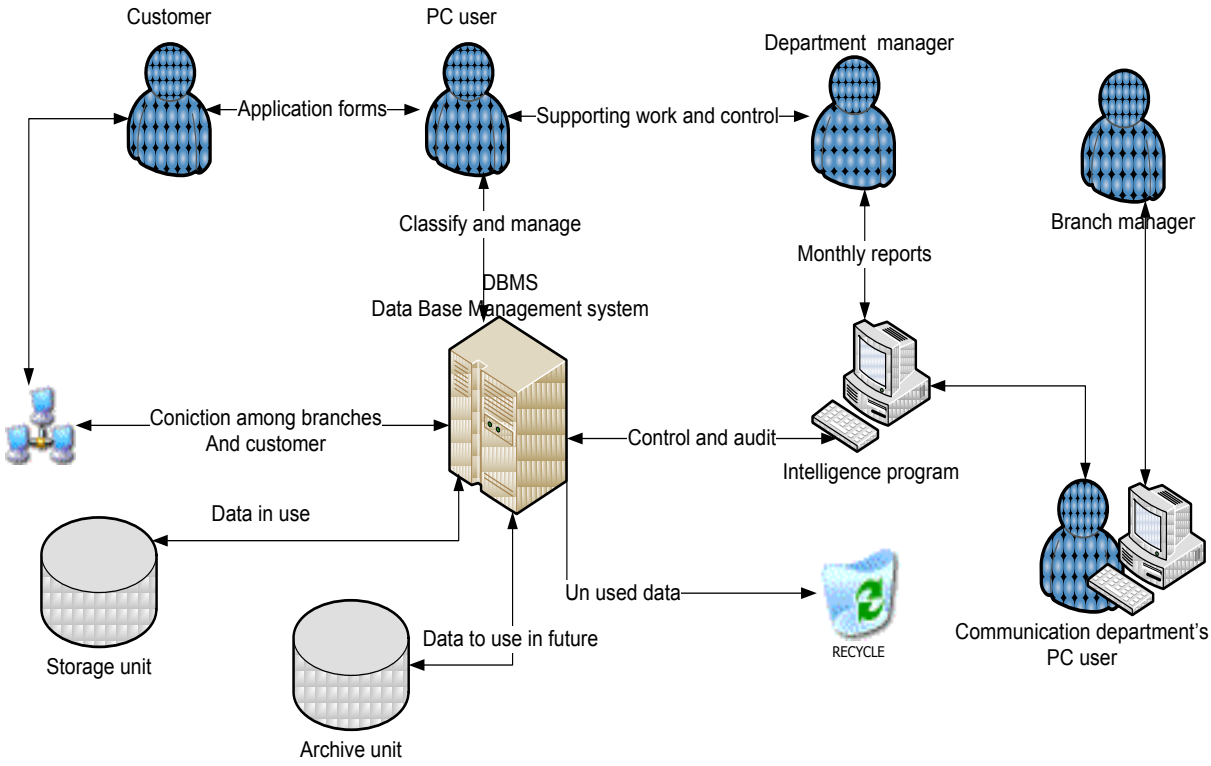

Figure 16 Processing Data Diagram of One Department inside Tripoli Branch

As we see The system started with handle or email request as an application form to determine the service needed by customer, the application form including the data which are important to the company’s business, and related to customer, the service process which received by the officer “the PC user “who’s will generate the service cooperating with the pc database system and supporting the service result “end product ”to be a legal work ,then will deliver it back to satisfy the customer’s need.

That was simple described of strategic work, but how we can keep data during these procedures safe in use.

Always there are three categories to deal with data, user, Dep- manager and technology if we look for the user there are two kinds of users.

In each department there is PC User ”PCU” also a customer which is a part of company’s system and considered as a data source, and starter of business.

The following figure show the relation between DLC & Users

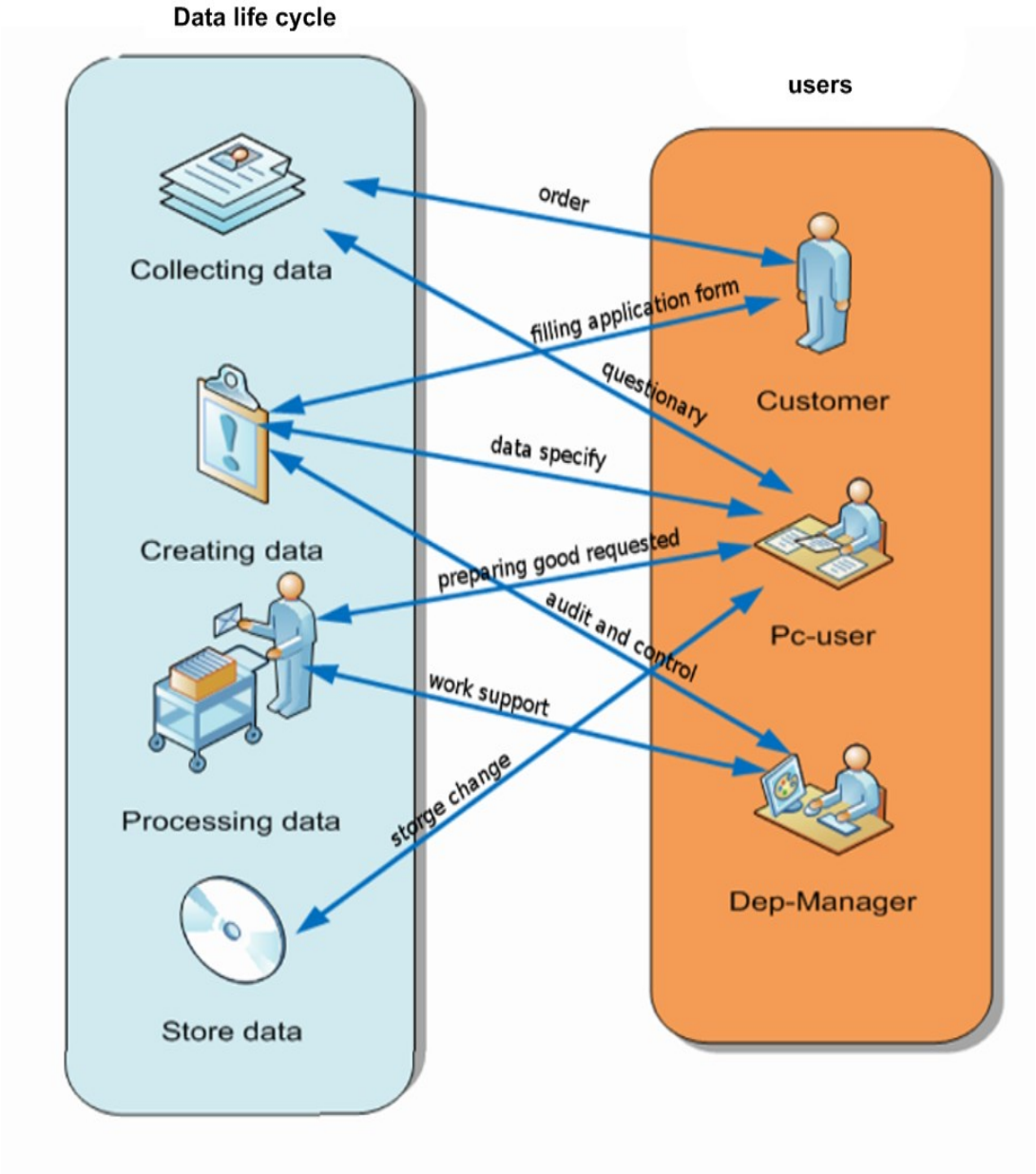

Figure 17 Relation between DLC &Users Categories

6.1.2. Scenario of business process analyze

Here I visited the company and I got the acceptance from the manager tome to feel free entering all departments and I made a list of questions to be answered from employee, following the scenario and writing the notes to be reforms in specific reports. Look for the question's list in appendix.

6.1.2.1. Collecting business's data

The relation In first step of business life cycle is between two kind of users "customer and the officer "the PCU" and that relation has two kind of tools first handling tool where customer goes to the company to meet the officer and filling data required by answering questions inside an application form chosen by kind of service need. And he will deliver it to the PCU by hand where he will correct any mistake that customer did.

The second way is a technical which is represented within an internet service where he will fill the application form and deliver it by an email through the internet and the next figure show that relation.

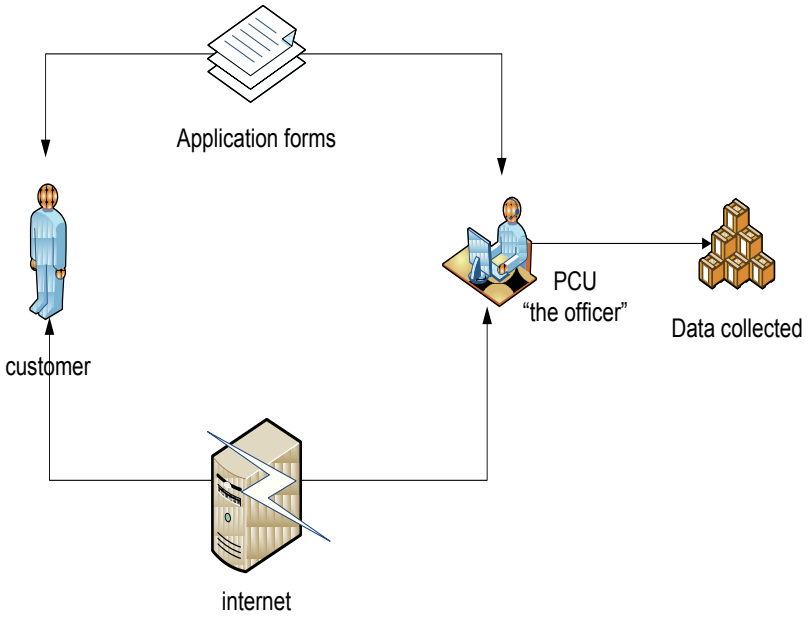

Figure 18 Collecting Data and Tools

- **Risk analysis**

As we see there are many data units in the collection process which have to analyze the possibility of risk incident in each one and its effects on the business:

➢ **Customer weakness points**

The customer is not one part of data process system of the business for the company but he is the resource of data and the business target for the company but also customers are the most targeted also by identity thieves and Computer hackers.

- **Entry data**

Customer is a human whose can make a mistake in entering data to the application form which will include his data, and He has to read and write carefully and to insure of data has to write that it is correct.

- **Insecure environment**

Customer use a variety of computing environment, while the company's network are secure but customer are not a user of the company's network.

Not all customers have a pc or internet. Where they are looking for friend's computers or for another network as internet café, where all are insecure and dangerous to use.

Customer has to use his privet PC or should insure that the network will use is secure, where cookies and the Internet surfing history can be left behind on Computers customer use. Also Files should be saved to removable media (USB keys, disks, Zip disks, external hard drives, CD-RWs, etc.) that can be carried.

- **Using email**

Customers mails are facility to get and often insecure that they are Unlocked and shared. Where a public mail boxes are great targets for identity thieves. For example Thieves will rifle through the mail to find personal information that Thieves can use to their advantage.

- **Application form weakness**

It is some questions the company designed for the customer to be answered to verify their data needed for business life.

These applications have to be designed carefully. That to be understandable for a customer and easy to fill it, that to avoidance giving bad or wrong data where will spend a time and money to fix that mistake.

As we said there to type a normal paper and an electronic application forms where gives the same service.

- **The Delivery weakness**

Data and services between the customers and the officer delivered by the two ways a handling way which is more secure way than the electronic way, which can be interrupted by thieves or hackers or to be deliver to the wrong address.

➢ **The officer**

For the officer in the part of collection data, There are limited points for risk incidence that, there are three points where the risk can be occur, these points are " password use, import & export procedure and the entry data ".

- **Password use**

The password is the access point to the company's system if some bad action occurred, it will cost the company much money and time, that they will lose data included in the machine or some thieves getting company's customer data and use it. Which will bring difficult situation to the company all that and more can be done from bad use of password.

The officer "PC user" should have own account and keep passwords in secret to maintain accountability. And changing the password at regular intervals, it will be sufficient to change passwords every month. The minimum length of passwords should be six characters and has to be including a numeric, alphabetic and other characters. And also has to Avoid temporary passwords unless absolutely necessary but if used change them at first Login.

Eider he should log off when leaving the equipment for some period of time.

- **Entry data weakness**

The officer's work will start as described before when receiving data delivered from customer with two rolls, handling and electronic rolls.

The officer leave's some mistake in his work if he doesn't read the received data carefully and insure, that the order type and features of the service's need, is wrote correctly from customer's side, which should be through enquiring the customer, that will avoid producing wrong products or service to customer.

- **Import & export procedure**

The officer has to import and export data from the server where fond DBS and from emails of customers and department's manager, which make possibility of harming system by viruses.

He must check data carriers against viruses and malicious software when importing them.

6.1.2.2. Creating business's data

Here we can notes in the figure number 18, that there are relation with three users a customer, PCU and Dep-manager.

The relation started with PCU where data collected from customer, will read it carefully to correct any mistake found by contacting back a customer then will prepare the contract if the situation is for new customer to be supported by the manager. And data in that time has been created to the form the company needs to start the process to produce the kind of service determined.

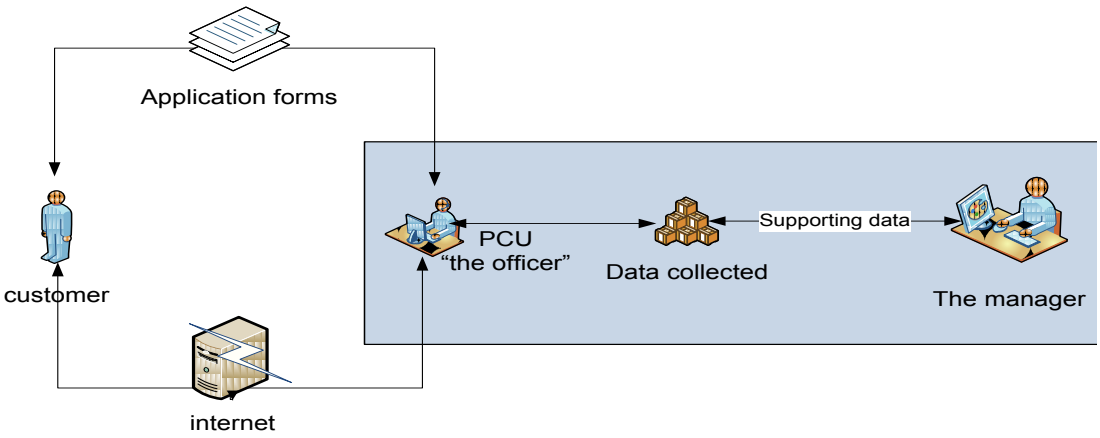

Figure 19 Creating Data

- **Risk analysis**

In this process there are two user of the system the officer which will formulate the data with help of customer's answer of queries to deliver for supporting by the other user the manager of the department which will receive the forms and make a decision if will accept this customer or not if they will produce a service to this customer or not. Delivery in this part is handle, which means no use of technical here.

In this process there is low level of possibility for risk incident, where it is dependent on the first process "collecting data" if it is done correctly and in secure way this process will be correct too.

The manager here is responsible for ensuring that adequate resources are available and allocated to maintaining security standards with respect will also make decisions about the penalties for breaches of security rolls.

6.1.2.3. Processing business's data

This stage about production process where there are two employs the officer and his manager; customer's data as material, company's business strategic (plan and rolls) and for sure the customer order.

In a general, as production described in [Bart Van Ark, 2000], A Production is a process of combining various material inputs (stuff) and immaterial (plans, know-how) in order to make something for consumption (the output). The methods of combining the inputs of production in the process of making output are called technology.

- **Risk analysis**

There is high level of risk rate caused by large number of steps and stages, which need by a production process and transform the last product to the customer's order.

To analyses the risk probability we have to study the user's weakness points where can the risk come from, and in this stage there are two users.

- **PC-user (officer) weakness point.**

If you decide to work in any company they will examine you to know your experience level in computer use, management and your last work and for sure your study's level, that all to be the company sure that you are able to understand the business process and your responsibility to avoid any loose of time by long training time or some simple technical damage which can interrupt or stop the business life cycle of the company.

Here we have to know the process the officer has to do, to know the points where data can be damaged, I visited the company for a month as an one of their employee and I been take three days with officer of life insurance, to be in live with him, to know the scenario of his working day.

The following figure describing that scenario as I found.

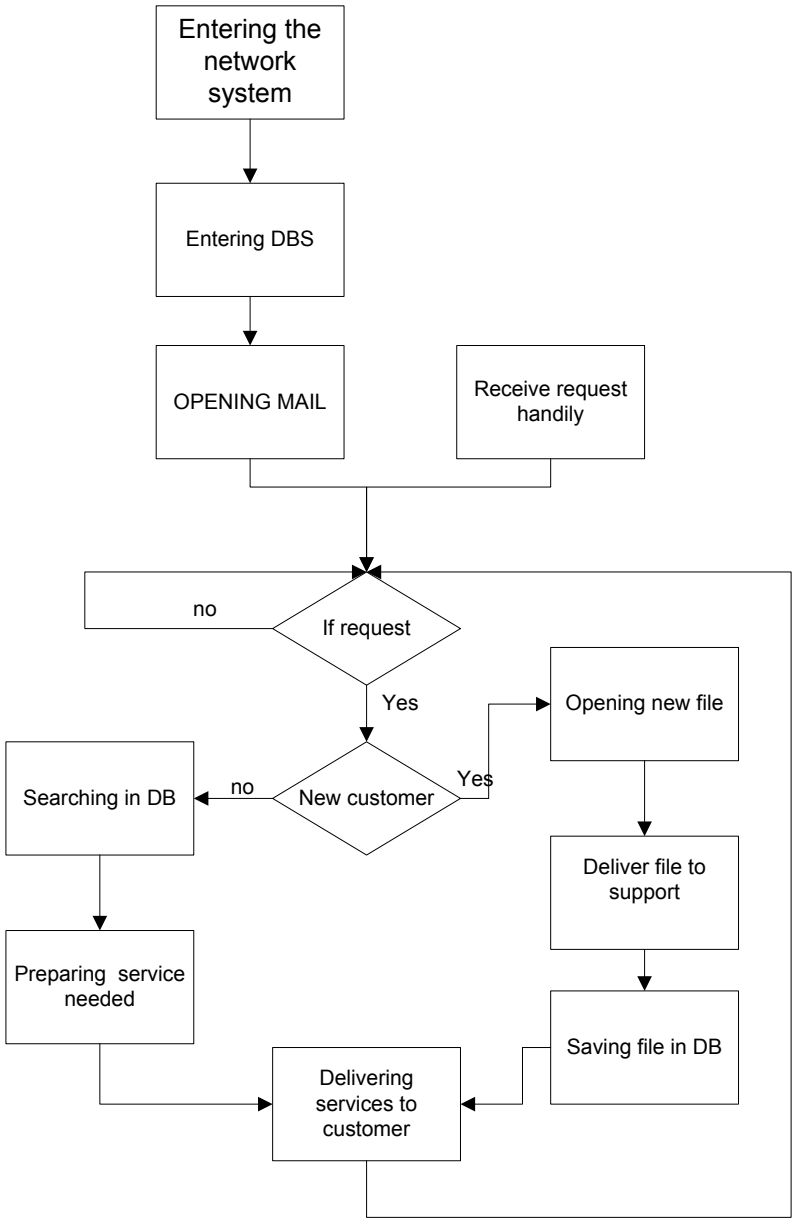

Figure 20 Scenario of PC User

In the simple we can display this scenario as “Receiving application and classify the kind of service needed, Comparing data with data in DBS if found, Measuring data if it is useful for a company, Will prepare situation report to the manager which will make a decision, Preparing contract between customer and company, Entering data to the DBS, And preparing information requested to the customer and manager and in the end delivering the products to customers“.

This was a simple and fast description of the production scenario. Now we will analyze the scenario to find the point of occurring risk and the security type should be there to disable risk incidence.

If we note the first three boxes are type of access control where user has an account. In each box there is a password “network system, data base management system and the email“. These keys are the access point to the data of the company which targeted by computer hackers and data thieves and have to be secured.

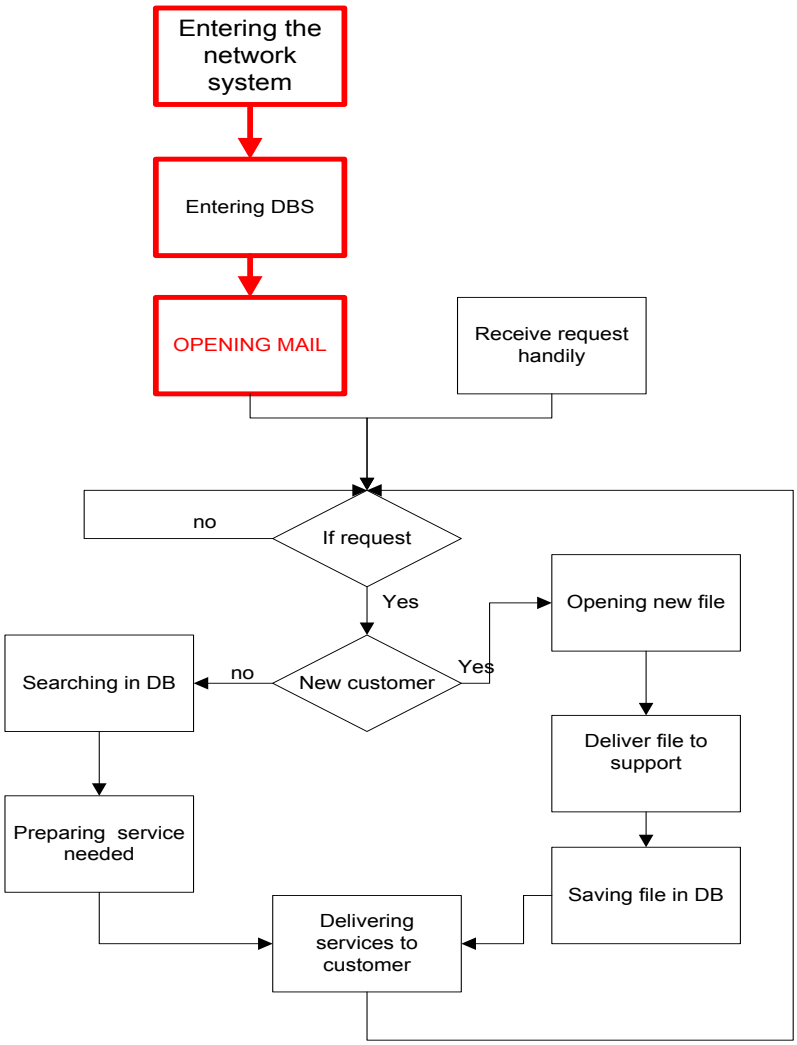

Figure 21 Access Control Process

Till Here the officer will collect data as we described before handily and from the email, we analyzed before

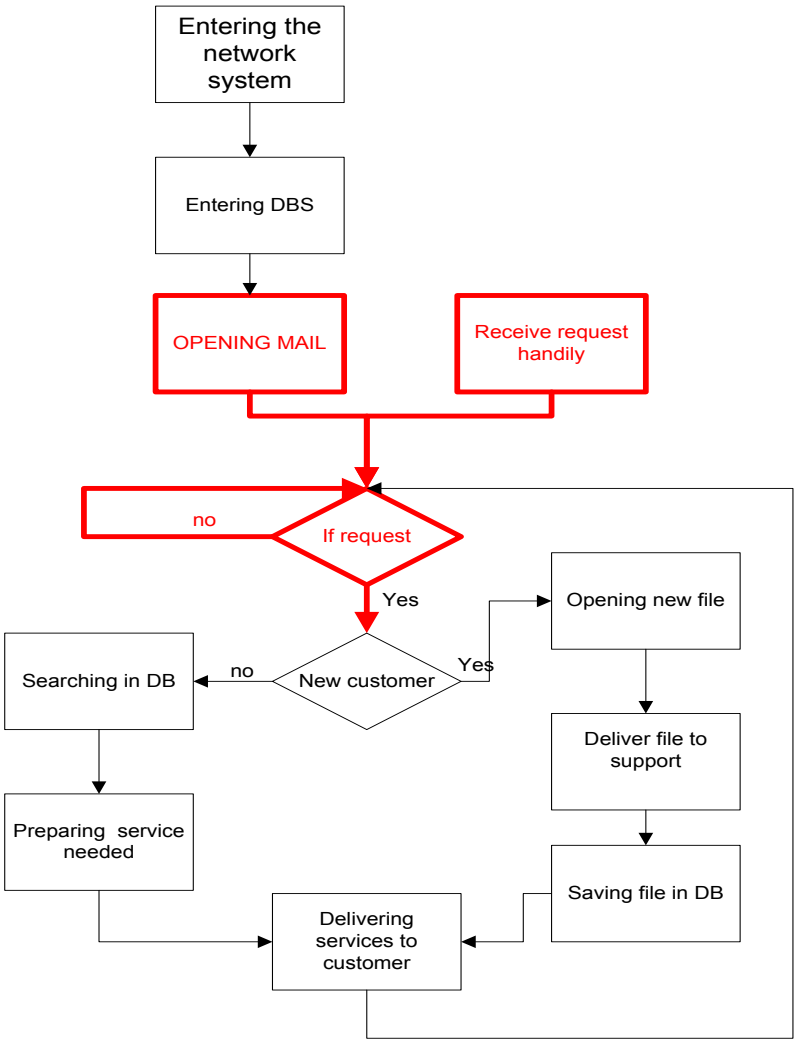

Figure 22 Collecting Data

This step is to work with the pc after classifying the kind of service then searching in data base if customer in there or not, that to determine if he is a new customer or ready in the system. It shows the second decision box.

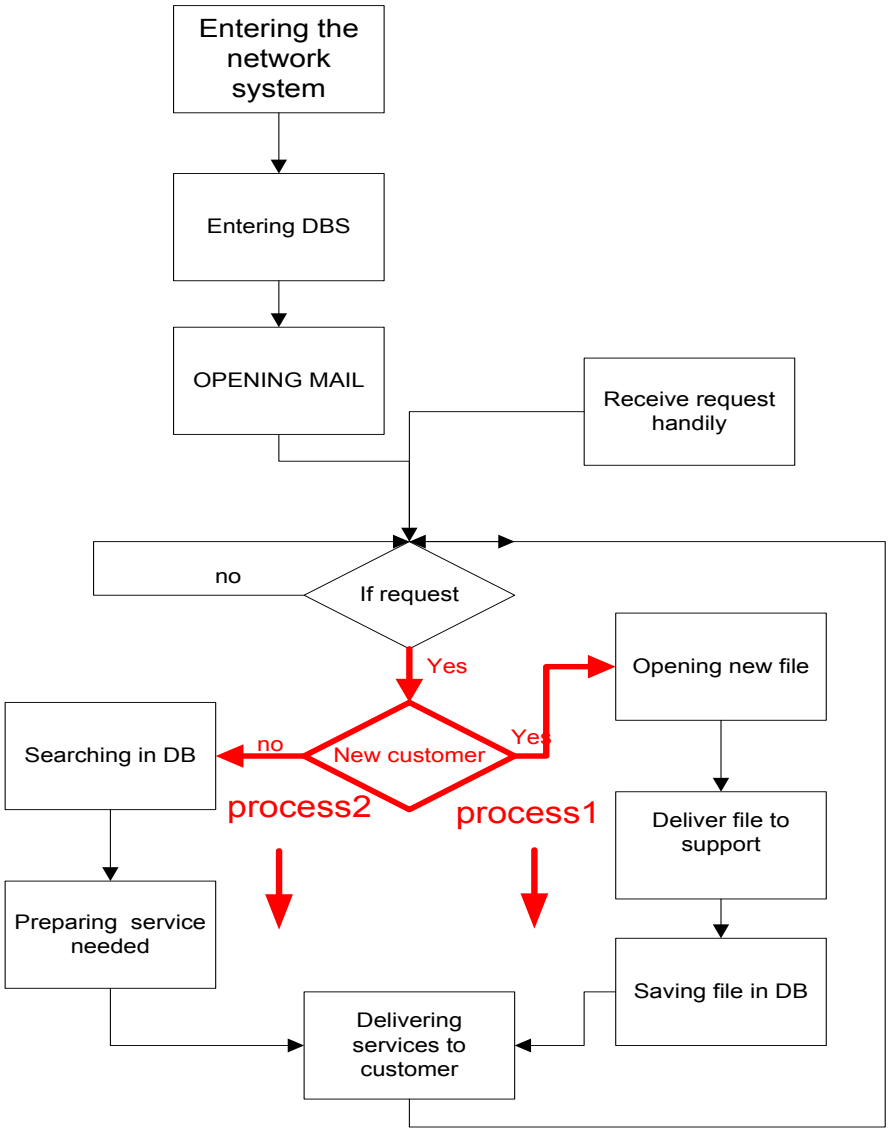

Figure 23 Classify Services Ordered

Process1 is a process where customer is new and not found in the system and there are three boxes in the scenario first is done by pc in database system and the second is a delivery type where the result of the pc will deliver to be support by Dep-manager the 3rd is going back to the PC and DBMS where decision has been taken to save data, by manager to provide a customer his order from last box.

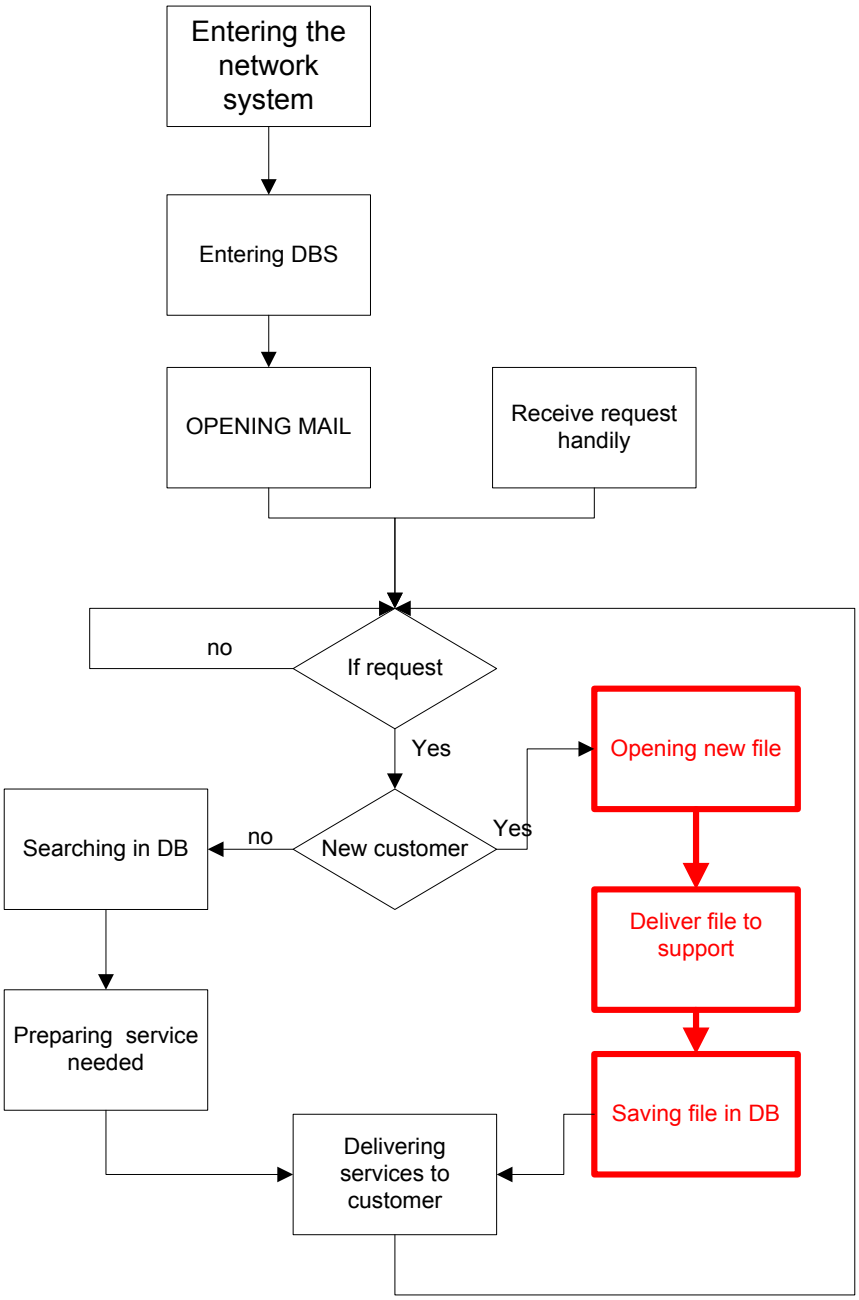

Figure 24 Process 1 of New Customer

Here the weakness point was in the delivery type, where officer leaves his office many times a day to the manager's office for supporting data which putting his office under the kindly thieves "the trusted people" who're able to enter his office with his knowledge.

Process2 as described following include two boxes first is to

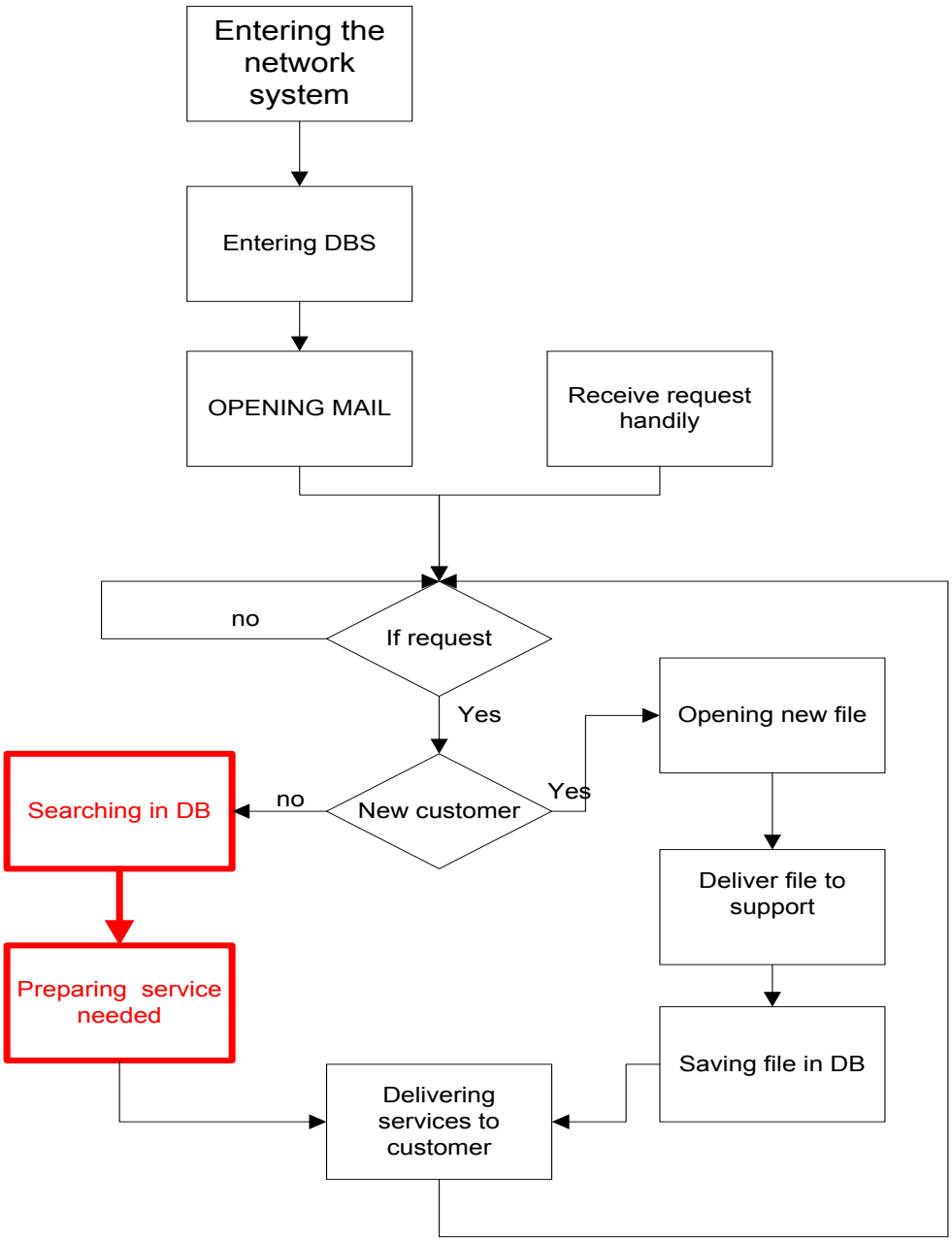

Figure 25 Process 2 of Old Customer

Fined the customers file in the data base system which stored before and including all his data and services got before, then will come the second box where will perform the latest pro ducts view “the end product” which will be delivered to the customer.

Here we can note that there is no supporting from manager side that all data collected in the customer's file are correct and supported before by the Dep-manager which meaning he is under service of company and he agreed with the low and policy of company, in that side the signature of the officer with his office stamp is enough to provide any future service of this department.

Here in the 2nd process the weakness in the expert and the mood of the officer knowledge and the mood "**"of the officer shows the level of the products "services" and the customer agreements.

***** Officer Mood,*** *when officer's mood is not good, means frowning he will not to do his job as well, officer has to control his feeling and shows the smiling face when he starts his work with customers, that, customers will agree with services because of the kind of transactions with officer*

The latest process box is delivering the end product from last processes points "the 1st and second process" to the customer. And there found two delivery type handling or by net. And here are some weakness points "the technical interrupt or wrong address point which summarized in (the internet problems) "

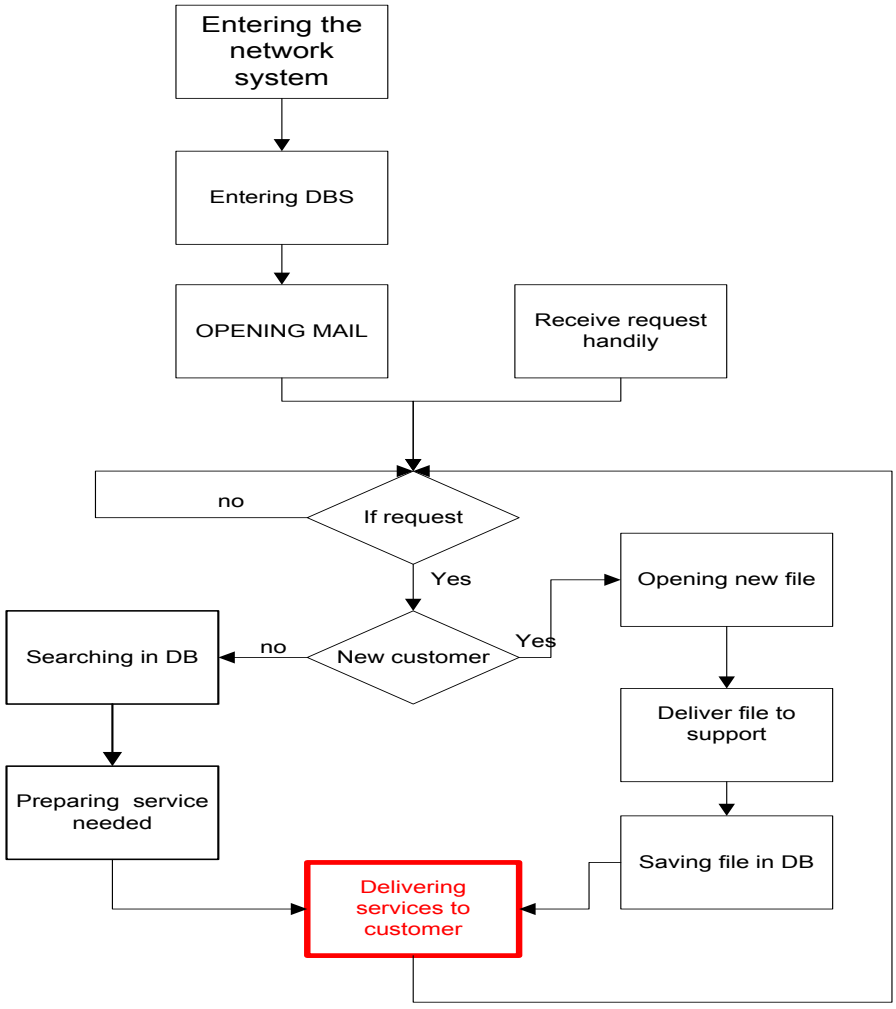

Figure 26 Delivering Final Product to Customer

6.1.2.4. Storing Data

There are two types of storage case, the archive and the technical way "servicers".

The Archive

Is the office where they have to keep all works done "ended" in handily way, that To cover any mistake can be done in future in the system or any problems done by officers, it is also used to audit the officers work

Technical Way

The strategic of storing data in the company is, that in each branch has to be one server where data stored and there are an uploading of that data to the central server of Tripoli branch, and that upload has to be every day in time determined by the manager of the main branch, And the following figure shows the communication between one branch and the main branch "Tripoli's branch" and how is going.

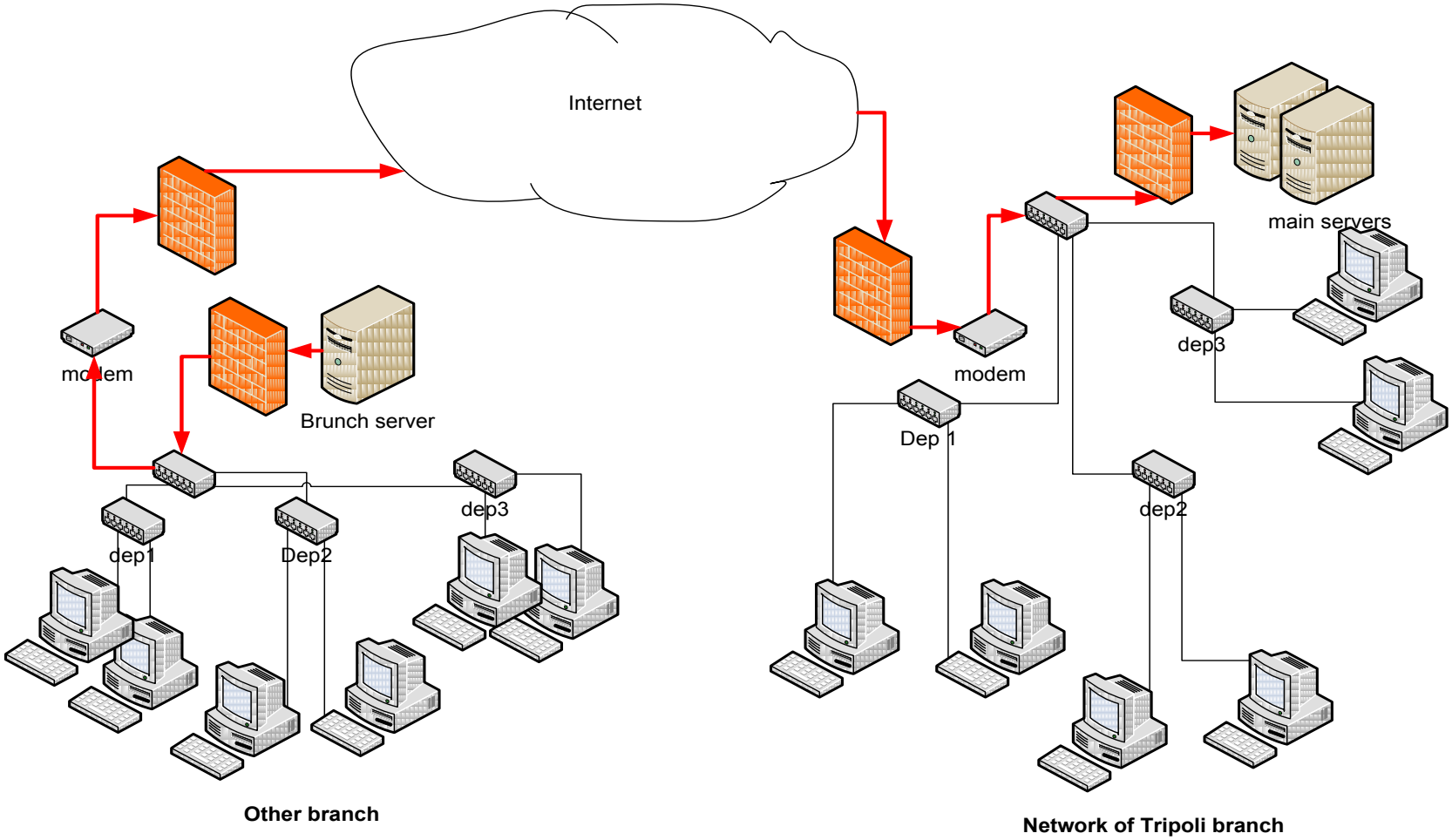

Figure 27 Uploading Data from Servers of Brunches to Server of Main Branch

- **Risk analysis**

In The archive there is more than a million file, which make the work there more complex, here thee experience in archiving required to decreasing the time lose, also the data is written in papers which can be destroyed by fire or water and some bad animals like a mouse from that we found that the place has to be away from the water and the fire and it should be a good built to keep animals away from it. There is one point that the worker has to respect the policy related to that "no smoking in and no other person entering inside and closing the room when leave it ,and taking care of the key and make it secure not to be stolen"

But in the other side the technical way, the problem from the officer in one point that he have to insure that he saved the data and it is the correct and the accepted data, the other points are technical weakness where it can be in uploading data by interrupt in the internet or some damage in any device of branch's network.

6.2. Implementing the model

6.2.1. Collecting security data required

Here from my consultation and the questioners I did, I summarized the data in three forms in: block form of management structure of (whole company, main branch, and life insurance department), processing scenario of life department as a standard department and in the end Threats and probability occurrence and outcomes. Look for the appendix stage no-A data no. 1, 2, 3, 4, and 5.

6.2.2. Creating security plan

From analyzing the system and the probability of risk incident I came out with policy list has to be accepted by top manager and the list of IT requirements in the way of security management then I came with the last operation level agreement. Look for the appendix stage no-B data no. 1, 2, and 3.

6.2.3. Processing security

This process has three sub activities and each one has its sub process these steps have to be done carefully.

6.2.3.1. Implementation

In this activity I have some steps from classifying and managing applications, implementing personal security, implementing security management and implementing access control.

a. Classifying and managing application

Here I determined, setup and install from the basket work and the IT statement, the requirements of each user from (hardware, software) and the following table shows the devices and software needed and the process I did.

IT Setup Statement			
date: 12/7/2010 to : 15/7/2010	place:	fire department of insurance company	**installation agreement Yes or No**
DATA USER	**HARDWARE**	**SOFTWARE**	
officer	PC with good features	windows 7	YES
		ms-office 2007	YES
		Application Process with Data Base Handy Backup Professional 6.9	YES
	hp printer 3 in one	identity software	YES
	router	identity software	YES
	cables		YES
	telephone	Express Talk VoIP Softphone	YES
	internet modem		YES
	server with good features	operating system Linux "ubuntu server 10.10" Handy Backup Server 6.9	YES
Dep-manager	PC with good features	windows 7	YES
		ESET NOD32 Antivirus 4	YES
		ms-office 2007	YES
		application process with data base	YES
		Handy Backup Professional 6.9	YES
	hp printer 3 in one	identity software	YES
	cables		YES
	telephone	Express Talk VoIP Softphone	YES

b. Implementing the personal security

Here I set all devices to be in the security level by using the firewall of windows and router and installing antivirus. Also I teach the users how they can keep their pc secure.

c. Security management

Here I distribute the security policy and display it to users, what is means and what they have to do and what they have not, and the consequences of violation the policy.

d. Implementing the access control

If we notes here are three type of access are: PC's-operating system, Access Application and Access Network, where I identified and authenticate all workstations and terminals. The following table shows that.

<table>
<tr><th colspan="5">Identify and Authenticate all Workstations and Terminals.</th></tr>
<tr><td>date: 12/7/2010</td><td>place:</td><td colspan="2">fire department of insurance company</td><td rowspan="2">installation agreement Yes or No</td></tr>
<tr><td>DATA USER</td><td colspan="2">Entity Type</td><td>DATA</td></tr>
<tr><td rowspan="2">officer</td><td colspan="2">MAC address</td><td>**.**.**.**.**.**.**.**</td><td>YES</td></tr>
<tr><td colspan="2">IP address</td><td>***.***.101.102</td><td>YES</td></tr>
<tr><td rowspan="2">Dep-manager</td><td colspan="2">MAC address</td><td>**.**.**.**.**.**.**.**</td><td rowspan="2">YES</td></tr>
<tr><td colspan="2">IP address</td><td>***.***.101.103</td></tr>
<tr><td rowspan="4">network details</td><td colspan="2">IP address</td><td>***.***.101.101</td><td>YES</td></tr>
<tr><td colspan="2">MASK address</td><td>***.***.101.100</td><td>YES</td></tr>
<tr><td colspan="2">BCAST address</td><td>255.255.255.0</td><td>YES</td></tr>
<tr><td colspan="2">PASSWORD</td><td>LIBYAN2010</td><td>YES</td></tr>
<tr><td rowspan="3">RUTER</td><td colspan="2" rowspan="3">FILLTER</td><td>MAC</td><td>YES</td></tr>
<tr><td>IP</td><td rowspan="2">YES</td></tr>
<tr><td>PASSWORD</td></tr>
<tr><td rowspan="5">SERVER</td><td colspan="2" rowspan="2">FILLTER</td><td>MAC</td><td>YES</td></tr>
<tr><td>IP</td><td>YES</td></tr>
<tr><td colspan="2" rowspan="3">PASSWORD</td><td>MANAGER **********
/Private</td><td>YES</td></tr>
<tr><td rowspan="2">USER **********
/Private</td><td>YES</td></tr>
<tr><td>YES</td></tr>
<tr><td></td><td></td><td></td></tr>
</table>

6.2.3.2. Evaluation

- Self Assessment

EXAMINATION REPORTS OF SECURITY AGREMENT		
PLACE: FIRE INSURANCE DEPARTMENT **DATE**: 20/07/2010		
Process type	**Minatory Result**	
right Use of Passwords	Allow	OK-100%
Network Entry	Allow	OK-100%
Server entry	Allow	OK-100%
Backup data	Allow	OK-100%
Restore data	Allow	OK-100%
Uploading data	Allow	OK-100%
Wrong Use of Passwords	Deny	OK-100%
Wrong Network Entry	Deny	OK-100%
Wrong Server entry	Deny	OK-100%
EXAMINATION REPORT OF USERS		
Careful	OK-80%	
Knowledge	OK-90%	
The consequences of violation of the laws	OK-100%	

- The other points of internal audit, external audit and audit in base of security incident it will done by time where the audit cannot be in one time of use it need at minimum three months to get result of the security implemented value.

6.2.3.3. Maintenance

Here depend on the agreement after receiving request from the organization to change the level of security agreement, the security agreement have to be changed and formulated To deal with flaws that have emerged over time, then implementing the new security agreement.

6.3. The Summary

The start date of my work was in 01/01/2010 with contacting the main branch to get the agreement about the consultation's time between me and the employee and the implementation started on 3rdJune2010.

The work took a long time because I was working alone in the project and it's in action from august 2010 and now and under control. Till now the result is good but the real result will be after one year at minimum. All the necessary data are collected in the appendix.

My future plan is to introduce my model to the trading area of my country and in the same time to improve the model by implementing it in more and different organizations type.

7. Conclusion

There are many practice models in the world of information technology like the British Standard and ITIL Information Technology Infrastructure Library, but they are not easy to implement.

The objective of my work is to improvement security management model which can be understandable for any organization used technology and planed to implement a security to secure their Data Resources and managed, also to be easy to implement and not to-much costly.

The base of the model is the Data Life Cycle management from collecting, creating, processing and storage, where I was producing the security management steps following DLC steps and formulating the security management as main DLC process.

Each process include some activity, where the collection include the organization's analyze of existing situation to find out data needed to create the security plan for implement, these data include three types, the management structure diagrams, scenario of business's process analyze and diagrams also the threat and probability occurrence and outcomes.

The management structure diagram can describe the type of communication and the responsibility of each person. And from the scenario analyze should formulated in diagrams to determine the devices and software required, also determining the weakness point in the strategic of processing data , in the end the determination of threat and probability occurrence and outcomes will be collected as list of history incident and weakness point determined by auditing employee behavior .

Creation process is the part where the plan of implementing security and managed and also include sub activities in creating three lists list of existing technology used and the technology required ,list of responsibility and the operational level agreement

Processes process is to implement evaluate and audit the plan as described in the method in chapter 3.

In my work I implemented the method on one Libyan company, named Libya Insurance Company LIC, and because the company is too big, I got agreement to implement the method on the main branch in Tripoli. And now is in action.

The implementation was too much difficult to me because they have no knowledge of security management, they were asking more than I could handle and I got a long time

of teaching and training them but in the end, it was all done after a long time and it is in the action. Last two months I got report that my project is still in action without any problem which was good news but the real result should be presented exactly after finishing one year in action. Then we can decide the quality's percentage of the model.

My future plan is to introduce my model to the trading area of my country and in the same time to improve the model by implementing it in more and different organizations type, also I am thinking to go through Smart Data Encryption.

8. Bibliography

- [Alison.C,2009] Alison Cartlidge Xansa-Steria , Mark Lillycrop.2009 “an introductory overview of ITIL”. v3 / auth. itSMF UK." The UK Chapter of the itSMF UK"- Vol. 3. ISBN 0-9551245-8-1.
- [Jacques. A,1999] Jacques A. Cazemier, Paul L. Overbeek, Louk M.C. Peters. 1999. “Best Practice for security management”. In United Kingdom. ISBN: 0 11 330014X
- [ABA, 2008] law American Bar Association .2008. “Data of Security Handbook. Section of Antitrust”. ABA. ISBN - 978-1-60442-047-0.
- [ISO/IEC17799, 2006] Timothy P.Layton.2006 “Information Security”. ISO/IEC17799 ISBN: 9780849370878
- [IGP, 2003] G. David Garson. 2003 “Public information technology: policyand management issues”. In US by Idea Group Publishing. ISBN: 1-59740-060-0.
- [Bart Van Ark, 2000] Bart Van Ark, Simon K. Kuipers, Gerard H.Kuper.2000 “Productivity, Technology and Economic Growth” in the Netherlands ISBN: 0-7923-7960-8.
- [Nina, 2009] Nina Godbole.2009. ”Information system security”. By Wiley India Pvt. Ltd. ISBN: 8126516925.
- [John .R.Vacca, 2009] John .R.Vacca.2009 in USA. Computer and Information Security. By Morgan Kaufmann Publishers is an imprint of Elsevier. ISBN: 978-0-12-374354-1.
- [Aycock John, 2011] Aycock John, University of Calgary. Spyware and Adware. 2011 In USA by Springer Science + Business Media. ISBN: 978-0-387-77740-5.
- [Thomas. p,2002] Thomas Peltier. Sep 29, 2002.”Information Security Fundamentals”. CSI Computer Security Institute. http://www.gocsi.com/ip.htm.
- [AVI, 2002] AVInformation. 2002. "Brief introduction to viruses, Trojans and worms". Anti-virus information. http://WWW.vanderbilt.edu/its/antivirus/AVInformation.html.
- [Storgesearch,2002] Storgesearch. Feb 4, 2002. “Developing a Disaster Recovery Procedure with Net Vault Backup Software” Online. http://www.storgesearch.com/bakboneart.html.
- [Oracle, 2007] Oracle. June 2007. “Information life cycle-management of business data”, An Oracle White Paper www.oracle.com/us/026964.pdf

- [DCT, 2005] Data Center technology. 2005" Information life-cycle management". Online. http://www.dell.com/downloads/global/power/ps3q05-20050118-Brisse.pdf
- [ITSC , 2003] Information Technology Support Center. 2003. "Best practices-security plus and policies".[Online 2008] www.itsc.state.md.us/info/internetsecurity/bestpractices/secpolicy.htm
- [SANS, 2003] Danchev Dancho. Sept 24, 2003. "Building and Implementing a Successful Information Security Policy" .SANS institute [Online] http://www.sans.org/rr/paper.pnp?id=418.
- [Bowden, 2003] Bowden Joel S. 2003"Security Policy 'what it is, and why?' the basics". SANS Institute [Online] www.sans.org/reading_room/whitepapers/policyissues/security-policy-basics_488
- [CIA, 2010] Central Intelligence Agency. 2010 "the World Factbook", [Online] Http://www.cia.gov/library/publications/the-world-factbook/gose/ly.html.
- [MS, 2009] Microsoft Windows Security "Computer Security",[Online]. http://www.microsoft.com/security/default.asp.
- [LIC, 2005] Libya Insurance Company (LIC). Tripoli 2005. "Internal journals". V 1, 2 and 3.
- [ITC, 2007] Information Technology and Communication Company (ITC). in Tripoli 2007. [Journal] Vol.15 E
- [ITC, 2006] Information Technology and Communication Company (ITC). in Tripoli 2006. [Journal] Vol.14C
- [Albright, 2002] Albright Jack G .2002 "The Basics of an IT Security Policy" SANS Institute [online]
- [FFIEC,2006]Federal Financial Institutions Examination Council .information security in July 2006.http://www.ffiec.gov/default.htm

9. Symbol Table

CAN-SPAM - Act. Designed to Protect American Customers

DB - Data Base

DBMS - Data Base Management System

DBS - Data Base System

DLC - Data Life Cycle

DoS - Denial Of Service

EDI - Electronic Data Interchange

EIU - Economist Intelligence Unit

FOIA - Freedom Of Information Act

FTP - File Transfer Protocol

GDP - Gross Domestic Product

GNP - Gross National Product

GSM - Global System For Mobile Communications

HR - Human Resource

HTML - Hyper Text Markup language

IP - Internet Protocol

IRC - Internet Relay Chat

IS - Information System

ISMS - Information Security Management System

ISP - Internet Service Provider

IT - Information Technology

ITC - Information Technology And Communication

ITIL - Information Technology Infrastructure Library

ITSMF - Information Technology Service Management Forum

LD - Libyan Dinar

LIC - Libya Insurance Company

NIDS - Network Intrusion Detection System

OGC - Office Government Commerce

PCU - Personal Computer User

ROI - Return On Investment

UN - Union Nation

WTO - World Trade Organization

10. Glossary

Availability - Ensuring that information and vital IT services are available when required.

Blended threats - Those that combine the characteristics of viruses, worms, Trojan horses, and any other malicious code designed to exploit system.

Botnet - Refers to a collection of compromised or zombie computers running malicious programs under the control infrastructure of remote commander.

British Standards - Code of Practice for Information Security Management.

CAN-SPAM - Act. Designed to protect American consumers from the continued receipt of mass spam message, establishes strict guidelines that commercial e-mailers must follow to continue their practices legally.

Confidentiality - Protecting sensitive information from unauthorized disclosure or intelligible interception.

Data security - The one of the most important assets. And protection of information assets is necessary to establish and maintain trust between a company and its customers.

Integrity - Safeguarding the accuracy and completeness of information and software.

Network intrusion Data that may be considered unauthorized occurring on a network.

Remote Access - The function of specifying access right to resource.

Spam - The common term used to describe junk e-mail.

Spyware - A type of malware that installed on computers and collects tittles bits of information at a time about users without users knowledge.

Trojan horses - Program or application that contains malicious code, unbeknownst to the victim.

Virus - A computer program designed to attach itself to host files and replicate repeatedly.

Worms - It is a computer program that self-replicates and spreads like a virus without necessarily infecting a host file.

11. Author's publications

- Musbah. A. Security Management of Student's Data. in MEKON 2007 VSB-TUO, Faculty of economics,2007 ISBN: 978-80-248-1458-2

- Musbah A. Designing Security Policy for Libya insurance company LIC, In Information Technology for praxi, Ostrava VSB-TU 2008, ISBN: 978-80-248-1841-2

- Musbah. A. Information Life Cycle Provide Security Policy .in MEKON 2009 VSB-TUO, Faculty of economics ,2009 ISBN:978-80-248-2013-2

- Musbah. A. Information Management Model within Data Life Cycle .In ECON Journal will appear in the beginning of the year 2012 VSB-TUO, Faculty of Economics.

12. Figure's Table